Social Network Modeling and Simulation of Integrated Resilient Command and Control (C2) in Contested Cyber Environments

Michael J. Lanham, Geoffrey P. Morgan, Kathleen M. Carley

December 9, 2011
CMU-ISR-11-120

Institute for Software Research
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Center for the Computational Analysis of Social and Organizational Systems
CASOS Technical Report.

This work was supported in part by George Mason University/AFRL/RISE under the grant Prime Award #: FA8750-08-2-0020; Sub Award # E2016762 (Resilient Architectures for Integrated C2 in a Contested Cyber Environment), by the Air Force Office of Sponsored Research (MURI: Computational Modeling of Cultural Dimensions in Adversary Organizations, FA9550-05-1-0388), George Mason University (CANS/Support for MULTI Modeling in Support of new Generation Nuclear Deterrence, E2023021), and Defense Threat Reduction Agency (Remote Capabilities Assessment, HDTRA11010102). Additional support was provided by the center for Computational Analysis of Social and Organizational Systems (CASOS). The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Air Force Office of Sponsored Research, Defense Threat Reduction Agency, the Department of Defense or the U.S. government.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
09 DEC 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Social Network Modeling and Simulation of Integrated Resilient Command and Control (C2) in Contested Cyber Environments	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,School of Computer Science,Institute for Software Research,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Department of Defense (DoD) leaders have a moral obligation to the nation to ensure that it can defend the nation and its interests. To meet this moral obligation, DoD leaders need ways of assessing the resilience of its forces?their ability to operate despite adversaries? actions. This report describes the application and analytic results of applying text mining and social network analysis to assessing resilient command and control (C2) of US Air Force Air Operations Centers (AOC) in a contested cyber environment. We also describe the progression from the static modeling to the construction and execution of a model with four doctrinally defined AOCs in an agent-based simulation named Construct. Through these modeling and simulation techniques, we have developed methods to assess impacts of simulated cyber attacks on the performance of single and multiple US Air Force (USAF) Air and Space Operations Centers (AOCs) and Operations Centers (OCs). With these assessments, analysts can make informed recommendations for developing mitigations to those attacks and provide simulations? results to assess the effectiveness of those mitigations.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**92**	

Keywords: Social Network Analysis, Social Network Modeling, Network Simulation, Command And Control, C2, Contested, Cyber

Abstract

Department of Defense (DoD) leaders have a moral obligation to the nation to ensure that it can defend the nation and its interests. To meet this moral obligation, DoD leaders need ways of assessing the resilience of its forces—their ability to operate despite adversaries' actions. This report describes the application and analytic results of applying text mining and social network analysis to assessing resilient command and control (C2) of US Air Force Air Operations Centers (AOC) in a contested cyber environment. We also describe the progression from the static modeling to the construction and execution of a model with four doctrinally defined AOCs in an agent-based simulation named Construct. Through these modeling and simulation techniques, we have developed methods to assess impacts of simulated cyber attacks on the performance of single and multiple US Air Force (USAF) Air and Space Operations Centers (AOCs) and Operations Centers (OCs). With these assessments, analysts can make informed recommendations for developing mitigations to those attacks and provide simulations' results to assess the effectiveness of those mitigations.

Table of Contents

1 Introduction

1.1 Motivation

Department of Defense (DoD) leaders have a moral obligation to the nation to ensure that it can defend the nation and its interests. To meet this moral obligation, DoD leaders need ways of assessing the resilience of its forces—their ability to operate despite adversaries' actions. They also need ways of assessing the abilities of the department's components to integrate their operations - to reduce the probability of working at cross-purposes with each other. Through the modeling and simulation techniques presented in this report, we have developed methods to assess impacts of simulated cyber attacks on the performance of single and multiple US Air Force (USAF) Air and Space Operations Centers (AOCs) and Operations Centers (OCs). With these assessments, analysts can make informed recommendations for developing mitigations to those attacks and proved simulations' results to assess the effectiveness of those mitigations.

This technical report expands on material submitted to AFRL in fulfillment of deliverable obligations. The final report (Levis, Carley, & Karsai, 2011) and this report describe the modeling and simulation efforts by researchers at Carnegie Mellon University. The first section provides background information for readers unfamiliar with DoD challenges, The second section describes the application and analytic results of applying text mining and social network analysis to assessing resilient C2 of an AOC in a contested cyber environment. The third section describes the progression from the static modeling to the construction and execution of model in an agent-based simulation. This portion of the research effort focused on the interaction of four (4) operations centers that we modeled as doctrinal AOCs.

The DoD is facing a multi-faceted set of threats to its cyberspace operations. In the face of these threats there has also been a growing realization within the DoD about its dependence on its Global Information Grid[1] (Joint Staff J7, 2010) This realization, publicly, began in earnest in 1998 with the discovery of a sustained attacks against DoD computer networks that the DoD named "Solar Sunrise"(Pike, 2011; Shackelford, 2009) and "Moonlight Maze" (Abreu, 2001). Though the attacks ultimately traced to non-state actors it provided the impetus to the creation of Joint Task Force Computer Network Defense (JTF-CND). Since the creation of JTF-CND, there have been numerous public calls-to-action from well-known security experts inside and outside the DoD. Each of those calls to action invariably identified different types of threats, the quantities of those threat types, and the strategic impacts of those threats. Each expert usually offered opinions about the quantity and significance of DoD shortfalls and made recommendations to improve security (Lynn, 2010; Webber, 2010).

[1] Joint Publication 1-02 Military Terms and Definitions defines the Global Information Grid as "The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems"

1.2 Evolution from JTF-CND to US Cyber Command

JTC-CND morphed over the years, as did the perceptions of responsibility to defend DoD's telecommunications networks. In 2008, the President, at the recommendation of the Secretary of Defense (SecDef) folded JTF-CND's descendent, JTF Global Network Operations, into a new subordinate unified joint command. This new command, US Cyber Command (USCYBERCOM) is a sub-unified command to US Strategic Command (USSTRATCOM). The President also folded USSTRATCOM's Joint Functional Component Command Network Warfare (JFCC NW) into CYBERCOM though he kept CYBERCOM as a sub-unified command reporting to USSTRATCOM. Finally, SecDef used his authority to temporarily appoint 4-star generals to recommend the President appoint the Director of the National Security Agency/Central Security Service (NSA/CSS) as the commander of USCYBERCOM (Gates, 2009). Figure 1 depicts a simplified version of the current task organization of the DoD for Cyberspace operations and begins the illustration of the number of stakeholders involved in assuring resiliency of command and control in contested cyber environments.

A short digression is appropriate to enumerate the specified missions of USCYBERCOM. The President assigned three primary missions to USCYBERCOM (Lynn, 2010), though he expressly did not change the underlying command authorities of combatant commanders enumerated in 10 U.S. Code *Armed Forces* ("Goldwater-Nichols Department of Defense Reorganization Act of 1986," 2010). The three specified USCYBERCOM missions are:

1. "Leads the day-to-day protection of all defense networks and supports military and counter-terrorism missions with operations in cyberspace.
2. Provides a clear and accountable way to marshal cyber warfare resources from across the military. A single chain of command runs from the U.S. president to the secretary of defense to the commander of Strategic Command to the commander of Cyber Command and on to individual military units around the world.
3. Work with a variety of partners inside and outside the U.S. government" (Gates, 2009).

These missions provide the rationale for the researchers to incorporate both USSTRATCOM's Global Operations Center (GOC) ("Strat OC" in Figure 1) and the 24th Air Force's Operations Center ("AFCyber OC" in Figure 1). The DoD's use of satellites as a primary and backup means of communications provides the rational for incorporating Joint Functional Component Command (JFCC) Space's (JFCC-Space) Operations Center (JSpOC) in the model ("Space AOC" in Figure 1). The regional combatant commander depicted in Figure 1 is US Central Command with their regional AOC provided under the command and control of Air Force Central (AFCENT) ("Regional AOC" in Figure 1). The vast majority of the US non-nuclear military capabilities are commanded and controlled through the regional combatant commanders: omitting a representative example would impoverish any modeling effort of contested cyber environments.

The numerous debates about the proper roles and functions of USCYBERCOM in the defense of telecommunications resources are well beyond the scope of this work. Instead we are focused on how our nation's current task organization supports the integration of multiple commands for a shared problem as well as supporting the resilience of that integration and internal command and control in a contested cyberspace environment

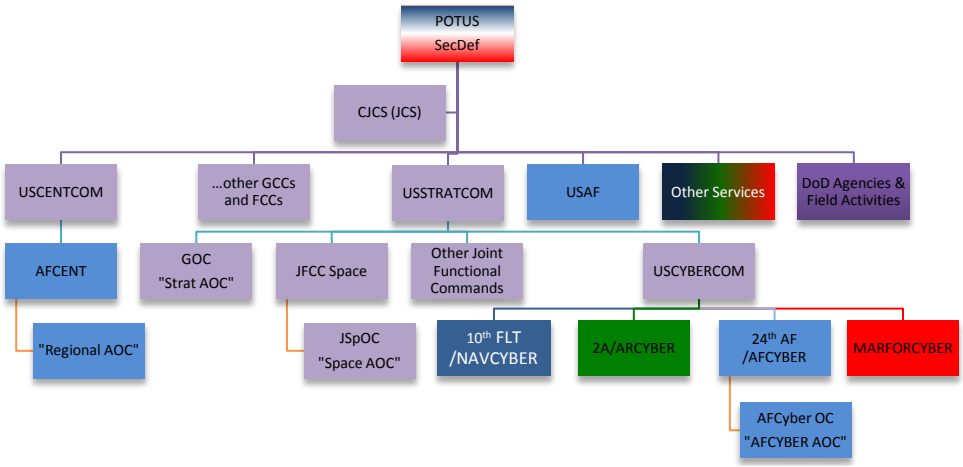

Figure 1 Simplified Task Organization of DoD for Cyberspace Operations

1.3 USAF Re-organization in support of cyberspace and other mission areas

Leading up to, and sometimes in parallel to, the decision to create USCYBERCOM, the USAF conducted its own reviews of "mission assurance" (Webber, 2010). USAF officials want to assure themselves and their field commanders of their organizational ability to conduct their missions, especially in the face of contested environments. Of particular concern has been assuring operational use of its telecommunications and IT systems. One of those many efforts by the USAF has been the creation of the 24th Air Force (24th AF), also known as US Air Force Cyber Command (AFCYBER). The 24th AF is the numbered AF the Secretary of the Air Force (SECAF) created to provide a service component command to USCYBERCOM.

The USAF has also been working to standardize the development and operations of AOCs around the globe. Part of that effort was the USAF decision to put an identifying nomenclature into its lexicon. The Air Force designated AOCs as AN/USQ-163 Falconer Weapon Systems(Paone, 2000). Some rationales for this USAF decision included:

- An effort to focus on *mission assurance* as a high-level task rather than pursuing perfect cyber defense (Parrish, 2011);
- A desire to standardize and systematize the acquisition of material solution components within the AOC;
- An attempt to treat a complex system of interacting personnel and equipment as a single engineering effort instead of a collection of material solutions and personnel training programs;
- A goal to reduce the disparities of people, processes, and material solutions in each AOC fielded by the USAF.

The USAF has developed hardened permanent AOCs for some of the Geographic Combatant Commands (GCC), deployable packages for regions without a hardened AOC, as well as functional AOCs for the functional combatant commands (FCC). The consolidation of so many capabilities into each Falconer AOC has made its dependence on cyberspace and telecommunications networks readily apparent to the AOC System Program Office (SPO) as well as the 24th AF. A goal of the AOC SPO, in coordination with (ICW) AFCYBER, is to mitigate the risks of dependence on telecommunications networks. That mitigation has to be

sufficient to assure various sets of leadership those AOCs can meet their missions' requirements in the face of contested cyberspace environments.

1.3.1 The AOC Mission

The AOC provides operational-level command and control (C2) of air and space forces as the focal point for planning, directing, and assessing air and space operations. To integrate air and space operations and accomplish its mission, the AOC coordinates closely with superior and subordinate C2 nodes, as well as the headquarters of other functional and Service component commands (USAF, 2005).

The AOC is the senior element of a Theater Air Control System (TACS). The TACS is composed of both airborne and ground-based C2 elements. To effectively integrate the TACS elements, the AOC develops and distributes numerous theater-wide guidance artifacts: Joint Air Operations Plan (JAOP); air operations directive (AOD); air defense plan (ADP); airspace control plan (ACP); airspace control order (ACO); air tasking order special instructions (ATO special instructions [SPINS]); tactical operations data (TACOPDAT); and operations task link (OPTASKLINK). These documents provide overarching direction to the TACS elements. The documents define roles, responsibilities, and authorities for decentralized execution (USAF, 2005).

1.3.2 Five Major Divisions, Matrix Support among 15 Functional Groups

There are five major divisions in the AOC as Figure 2 illustrates. The model used in this study incorporates all these divisions as well as the functional groups shown in the figure.

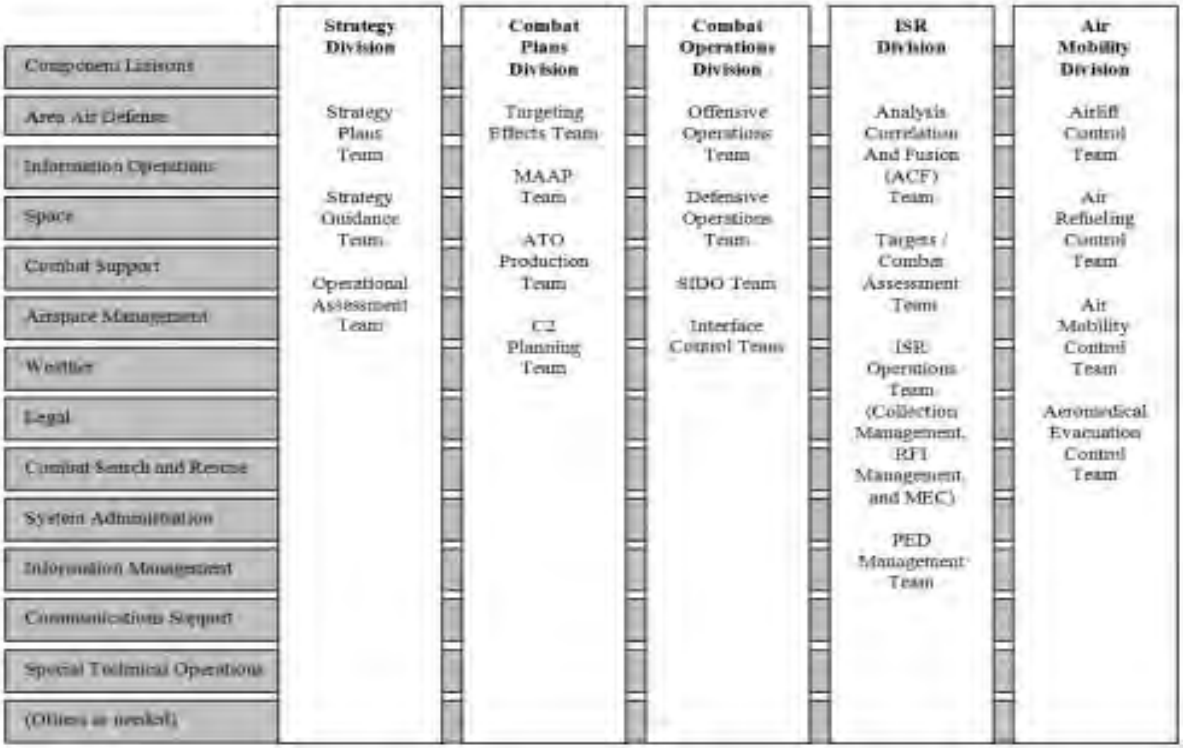

Figure 2 AOC Organization (USAF, 2005)

1.3.3 AOCs and the Cyberspace Chain of Command

The AOCs are not directly under the command of USCYBERCOM or the 24th AF/AFCYBER as Figure 1 illustrates. Given the research effort's assumptions the researchers assessed it was prudent and reasonable to include AFCyber's Operations Center. We made the simplifying assumption for the model that it has the same configuration as a doctrinally-defined AOC. We also omitted the numerous ways information, technical directives, alerts and other information that can flow to the AOCs. Examples of those complicating factors include: Administrative Control (ADCON) channels; Network Operations (NetOps) tasking and reporting channels; Information Assurance channels; Computer Network Defense Service Provider (CND-SP) channels; and the USAF's. two Integrated Network Operations and Security Centers (I-NOSCs) under the 67th Network Warfare Wing (24th Air Force Public Affairs, 2011). These channels can lead to ambiguous conditions where various elements of the Combatant Commands, the USAF as a Military Department, and the 24th Air Force all perceive that they have the legitimate and legal authority to direct actions of units, personnel, and resources.

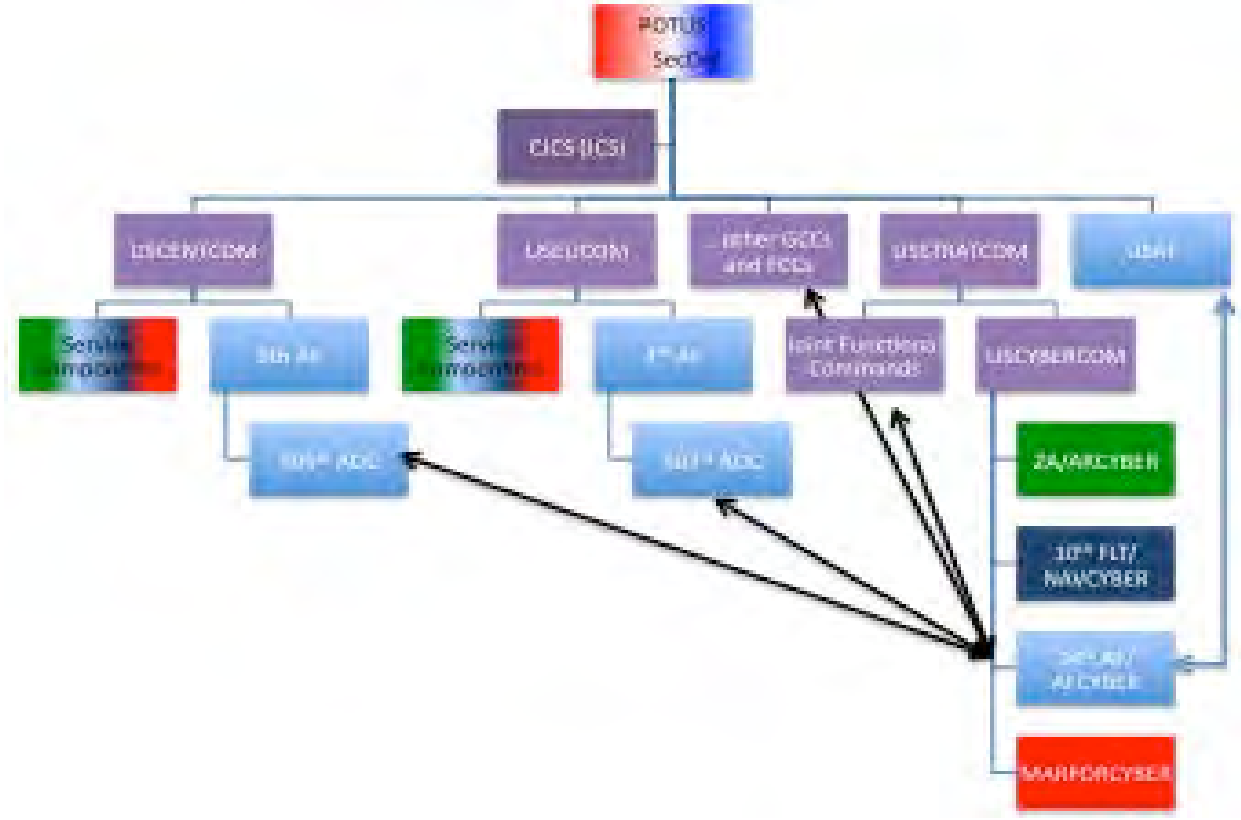

Figure 3 Course-Grained view of 24th AF interaction with AOCs' Net Defense (NetD) and Network Operations (NetOps) Cells. The line from USAF to AFCYBER represents Administrative Control (ADCON) as well as Service-Specific NetOps.

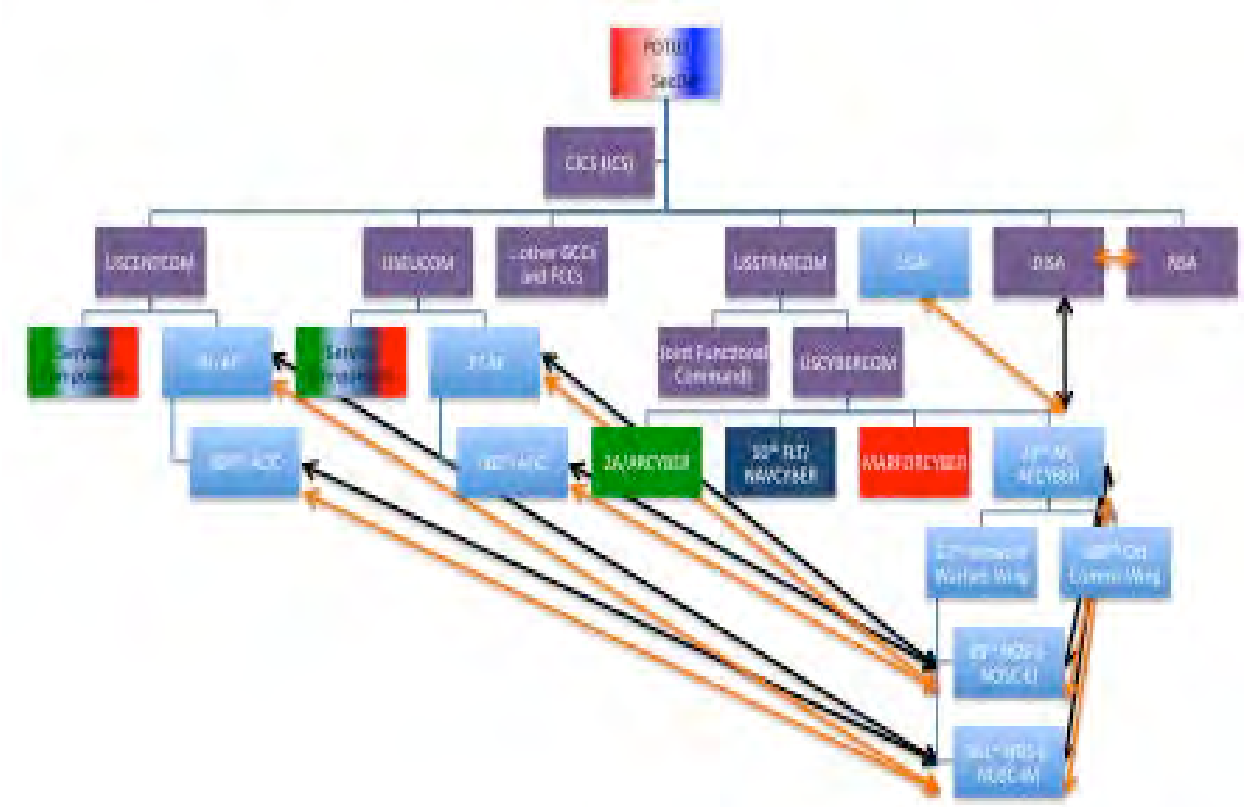

Figure 4 Computer Network Defense Service Provider (CND-SP) lines of influence (black) between 24th AF and USAF elements in other COCOMs. Information Assurance (IA) lines of communication (orange) between NSA, DISA, USAF, 24th AF and other AF elements not under the command and control of 24th AF.

The existence of these lines of influence has the potential for affecting the mission assurance capabilities of AOCs. With realistic modeling and simulations of the AOC, and its interactions with external entities, researchers can explore the limits of that potential. It is feasible that the potential is small enough to cause no concern for the affected COCOM(s). It is also feasible that the potential varies over phases of campaigns and operations. With varying degrees of importance, the COCOM(s) and Military Departments, as well as USCYBERCOM can exercise varying levels of concern and control in a conditions-based, well-rehearsed basis rather than a one-size-fits-all basis. This project did not model of these lines of influence and defers that effort to future work.

1.3.4 What does it mean to degrade an AOC?

The research effort focuses on comparisons between a baseline model and various combinations of IT systems operating in a degraded state and impacting the operations of the AOCs. In this way, we can meet support measuring the AOCs' *network resilience* as defined in (Committee on National Security Systems (CNSS), 2010):

A computing infrastructure that provides continuous business operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands.

The DoD has developed a five-part definition of information assurance that helped the researchers narrow the scope of the experiments to reflect a contested cyber environment. The five part definition emphasizes key effects that friendly forces must ensure: availability; integrity; confidentiality; authentication, and non-repudiation (Committee on National Security Systems (CNSS), 2010; Joint Staff J7, 2010). By using these five broad labels, the researchers and readers are relieved of the necessity of modeling and simulating the literally thousands of techniques by which US forces can have a reduction or total loss of their cyberspace capabilities.

US Joint doctrine usually defines degrade as a mission task for friendly units to execute against an adversary. The task is simply "to reduce the effectiveness or efficiency of [the] adversary…"(Joint Staff J3, 2006, pp. I-9). Military planners apply the task in whatever domain they are operating within (e.g., artillery planners will want to degrade enemy forces in range of their cannons, air attack planners will want to degrade adversary air defense capabilities, computer network attack planners aim to deny, degrade or disrupt (Committee on National Security Systems (CNSS), 2010) the system(s) and network(s) the enemy is using to achieve some friendly operational effect(s)). Degradation can occur at any level from 0 to 100%, can be a first or nth order effect of some cause, as well as intentional and non-intentional. Importantly, degradation can be self-inflicted as well as inflicted by adversaries and Mother Nature.

An AOC can experience degraded operations through a variety of means: blocking or reducing the effectiveness of communications to external entities (e.g., loss or reduction in availability); loss of confidence in authenticity and accuracy (e.g., loss of integrity) in transmitted orders and information; loss of confidence by external units that the AOC has situational awareness of their operating environment. Degraded operations can also occur through loss of personnel and equipment, over-extension of personnel (e.g., too many expectations, not enough resources to meet them all), as well as any number of other situations that would prevent the AOC from operating as the USAF designed and the COCOM commander expects. Examples of ways degradation could occur are in the table below.

Table 1 Example generalized methods of affecting AOC IT systems

General method	Unclassified Systems / Networks	Classified Systems/ Networks	Information Assurance Component
'Back-hoe' attack (e.g., deliberate or non-deliberate physical destruction of land-lines)	X	X	Availability
Natural Events (e.g., earthquakes, tsunamis, tornados, sandstorms, solar flares)	X	X	Availability
DDoS	X (e.g., targeted systems; network segments supporting those systems)	X (e.g., against the supporting commercial carrier's network segment transporting the encrypted link(s), unless somehow within the crypto-graphic separation	Availability
Mal-ware (e.g., Virus, worms, keyboard loggers)	X (e.g., on targeted systems, targets of opportunity)	X (first infection usually through transfer from a different network(s), subsequent infections propagate as on any other network)	Availability, Confidentiality, Integrity, Authentication
Remote Access / Control	X (e.g., bot-nets, privilege escalation and propagation)	X (e.g., delayed/time-lag due to crypto-separation of networks; real-time through access to crypto-separated terminal(s); real-time through some bypass of crypto-separation)	Confidentiality, Integrity Non-repudiation Authentication
Infrastructure subversion (e.g., control of one or more components of commercial infrastructure	X (e.g., telephone company central offices; underground cable conduits/tunnels; microwave/LOS transmission towers)	X (e.g., unless somehow able to defeat deployed cryptographic protection, compromise of traffic would be limited to enriching adversaries ELINT take as well as loss of availability of the	Availability; Confidentiality, Integrity, and Authentication for unencrypted links

		transmission path of the encrypted data stream)	

1.4 Shortfalls in Experiment Support For Organizational Structures, Policies, Technologies and People to Improve Resilience

Prior to creation of USCYBERCOM, responsibility for cyberspace operations was spread out across a number of organizations: Defense Information Systems Agency (DISA), JTF-GNO, JFCC-NW, Military Departments (MILDEPS), Combatant Commanders (COCOMS), as well as DoD Agencies and Field Activities. With the creation of USCYBERCOM, JTF-GNO and JFCC-NW have now merged into a single sub-unified command as discussed above. Each MILDEP is pursuing distinctly different regimes in terms of centralization, command and control, configuration control, and other aspects of cyberspace operations. Those various pursuits illustrate a key point: re-organizing large organizations (DoD-level), re-organizing inter-organizational behavior, authoring new policies and directives to guide new interactions and responsibilities, as well as re-allocating missions, resources, infrastructure, and personnel are all different ways of working toward the same goals—though it is clear each method has its own interests, stakeholders, constituents, adherents, and publicists.

The general paucity of simulations, or other applicable methods, for studying and predicting outcomes of reorganizations complicates the DoD's efforts. To make meaningful comparisons between the status quo and experimental futures, there must be more robust efforts at modeling, simulating, and studying friendly forces. Critical tasks for the simulations and evidence-based research communities include understanding the interplay of friendly variables, being able to make predictions and run experiments to confirm or deny the predictions, and being able to communicate the results of those experiments and predictions. This paper is a step in the direction of providing repeatable, large-scale simulations of DoD organizations conducting cyberspace operations as well as the MILDEPs training, manning and equipping of forces to operate in contested cyber environments.

This research effort focused on the interaction of four (4) operations centers that we chose to model uniformly as a doctrinal AN/USQ-163 Falconer Weapon System. Each of these operations centers (which we'll refer to as AOCs in the remainder of this work) is responsible for receiving, analyzing, processing and implementing orders from their respective Headquarters. CMU has made the assumption that the relevant higher headquarters have already integrated their respective tasks into a synchronized and coordinated higher-echelon operations order (OPORD). Figure 2 depicts the nested research efforts between George Mason University (GMU) and CMU.

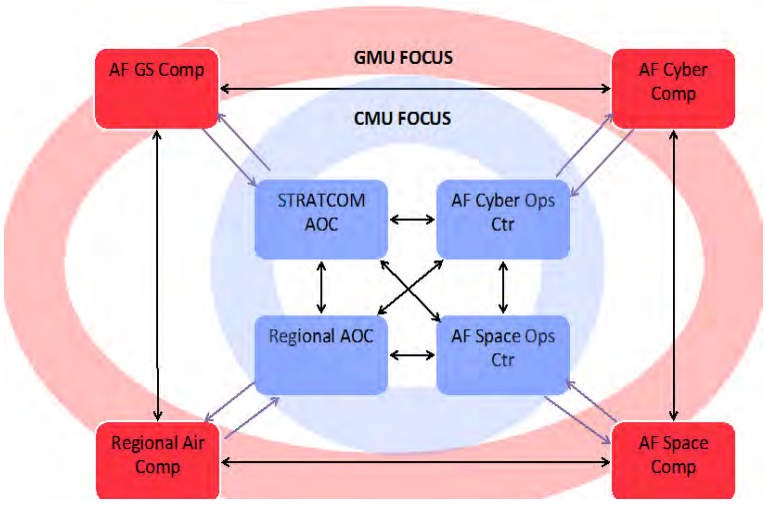

Figure 5 Depiction of relationship of research between GMU & CMU

2 Social Network Modeling, Text-mining & Data-to-Model (D2M) Processes

2.1 Social Network Data Description

The data for this project is from four (4) source documents representing a mix of Joint and USAF service doctrine. These documents are available to the public and are therefore ideal to support unrestricted research. Their availability however does come with a few facts that future researchers and readers need to remain aware of: the documents are written and edited by teams of individuals; the documents' authors consistently state that the doctrine they are writing is a common point of departure for fielded AOCs—that no AOC is structured exactly like depicted nor performs in the same manner as conveyed; the documents have a number of acronyms that have multiple original meanings even in such a small data set.

1. Joint Publication (JP) 1-02 Department of Defense Dictionary of Military and Associated Terms
2. Air Force Instruction (AFI) 13-1AOC, Operational Procedures - Air and Space Operations Center (AOC)
3. Air Force Tactics Techniques and Procedures (AFTTP) 13-3.2 AOC, Operational Employment Procedures - Air and Space Operations Center (AOC)
4. Air Force Forces (AFFOR) and Air and Space Operations Center (AOC) (Geographic) (AFFOR/AOC-G) Universal Task List (UTL), Universal Joint Task List (UJTL), Mission Essential Task List (METL).

2.2 Text-mining, Automap, and the Data-to-Model (D2M) Process

AutoMap is a Network Text Analysis tool that extracts concepts from a variety of unstructured text sources(K. M. Carley, Columbus, Bigrigg, & Kunkel, 2011).. A concept is a single idea (e.g., person, location, resource, belief, event, organization, and role) represented in a data corpus by a single word or phrase. AutoMap creates a map of concepts connected to each other through computerized application of a set of coding rules. Coding rules consist of, among other things, pre-processing in the form of removal of numbers, de-capitalization; thesaurus transformation of word forms to canonical forms (e.g., "United States" and "the United States of America" to "United_States"); concept generalization (e.g., "attack", "assault", "strike", "bomb", "shoot" all generalize to "attack"); and delete lists (e.g., deliberate deletion of concepts not relevant to the research question)(K. M. Carley, Columbus, Bigrigg, et al., 2011).. Concepts authors insert into documents appear in final products unless deleted by the researchers' delete lists. Choosing which nodes to retain in the model is a subjective function of the researchers and the research question(s) at hand. The encoding scheme the researchers used to create the project thesaurus is in – Encoding Scheme for Ontological Classification.

The concept maps the network text analysis tool (AutoMap) generates represent the semantic distance and links between words in the input corpus and helps researchers identify which node set(s) individual concepts may belong to. AutoMap links nodes to other nodes based on sliding windows. The researcher can choose to various lengths/sizes for the sliding window, to have the window cross sentence or paragraph boundaries, and even maintain a count of how many times the window has crossed sentence/paragraph boundaries. Each of these decisions will cause a slightly different output network, especially in network density measures.

The source documents had a robust collection of diagrams, tables, and lists. To harvest information from these materials, the supplementary materials must be either turned into a

textual form AutoMap can process or a researcher must manually create nodes and links in ORA. We choose to transcribe select diagrams (e.g., Figure 2) into text files to allow subsequent incorporation into the D2M process. The transcribed text file had simple declarative sentences, using Figure 2 as the exemplar, such as, "The AOC has a strategy division." This methodology allows the team to add or change source documents. An alternative methodology could have been building the networks representing the supplementary material by hand and merging those networks with AutoMap's outputs. We followed the same declarative sentence method to correct AutoMap-created isolates. For lists, we created complete sentences with the doer of the action and the action itself within each the sentence. Lists would take the form of the following: "The combat plans division makes the ATO. The combat plans division distributes the ATO. The combat plans division monitors the execution of the ATO." CMU's Center for Computational Analysis of Social and Organizational Systems (CASOS) continues to develop heuristics and test ways of text mining lists, tables, and diagrams and meaningfully add their content into network models.

After initial results, we collapsed the encoding scheme further by consolidating agents, organizations, and roles into the agent node class.

Table 2 Node class sizes before transcribing figures, manually correcting isolates, collapsing roles and organizations into agent node set

Node class	Size
organization	333
task	376
knowledge	566
location	154
resource	197
role	202
belief	66
action	28
agent	237
event	16

Table 3 Node class sizes after transcribing figures, manually correcting isolates, collapsing roles and organizations into agent node set

Node class	Size
—	—
task	383
knowledge	579
location	154
resource	199
—	—
belief	66
action	28
agent	957
event	21

2.2.1 ORA Modifications to Automap Output

On initial review of the network files AutoMap generated, it became apparent that additional data 'cleaning' was necessary prior to generating more in-depth analysis. We merged agents, organizations, and roles into a single *agent* node class—we used an attribute to differentiate the various kinds of agents (e.g., 'org', 'agent', 'role'). We also discovered that the initial generous retention of organizations caused a shift in focus of the model from being AOC-centric to AOC-within-DoD.

When we retained the specific entries for every non-AOC organization in the input files, the key entity reports had more than 50% of their entries as non-AOC entities. Immediate impact reports also gave no suggestive or meaningful results as all the non-AOC agents overwhelmed the agents within the AOC. It's a discussion point for others to assess if the doctrinal sources contain too much information addressing the interactions between the AOCs and all the organizations it can/should/must communicate with. For our purposes of evaluating the AOC itself, we needed to do some more consolidation and abstraction within the model. We

consolidate all non-AOC DoD organizations into a single DoD_orgs node, and did the same for US Government nodes, Non-governmental nodes.

Table 2 and Table 3 show the quantities of each node class before and after the collapse.

Additionally, we used ORA's ability to transform the resultant meta-network to remove, based on the entire network, all isolates and pendants. When we base removal on the entire network, it means ORA only deletes nodes that are connected to no other node of any type—it's feasible that an agent node is connected to no other agents when connected to tasks and resources. Nodes that fit that situation remained in our model. We also created a reduced form network as well as symmetrized the network. A reduced form network means that we collapse two networks into a single network (e.g., Agent x Task and Task x Agent get collapsed into a single Agent x Task network) before symmetrizing the resultant network.

These transformations reduced the number of links by 17% while the transcription of figures to diagrams and manual correction of isolates improved total density by 79%. Through this combination of turning pictures into words for mapping, breaking lists into their constituent parts, and returning to source documents to manually correct isolates, we were able to refine and clarify the generated networks without doing violence to the model.

Table 4 Meta-Network General Statistics before collapsing, reducing, and symmetrizing

Statistic	Value
Node class Count	10
Node Count	2,175
Link Count	68,968
Network Count	110
Total density	0.0148

Table 5 Meta-Network General Statistics after collapsing, reducing, and symmetrizing

Statistic	Value
Node class Count	8
Node Count	1,984
Link Count	57,818
Network Count	36
Total density	0.0265

2.3 Social Network Analysis Using ORA

2.3.1 ORA Visualization of the AutoMap-generated Network

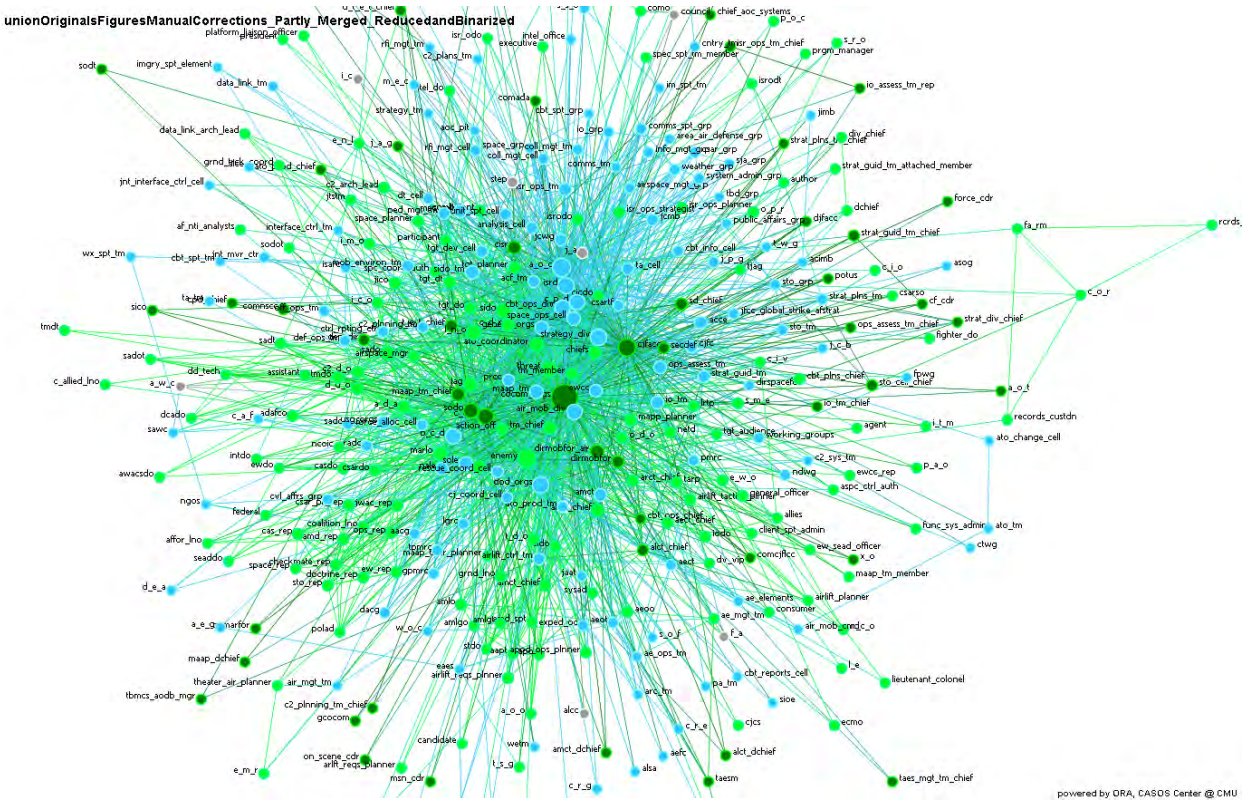

Table 6

Lacks an Attribute value
org
person
role

Figure 6 Agent x Agent network sized by Centrality, Authority, colored by the 'category' of agent, removed isolates and pendants, and zoomed in

The agent x agent network depicted in Figure 6 reflects the output of the data collection, cleaning, and refining steps discussed above. The AOC as a distinct entity is the blue circle with white background in the approximate center of the diagram. Because the source documents included references to many entities beyond the organizational lines of an AOC, the diagram is significantly more complicated than it might otherwise have been.

Figure 7 below shows 85 nodes representing the AOC Divisions, and their respective teams and cells, the AOC Functional Groups, and Elements co-located with the AOCs (e.g., Liaison Officers (LNOs)). Nodes remained sized by *Centrality*, *Authority* and we also removed isolates and pendants from the graphic. The color legend for both graphs is shown in Table 6.

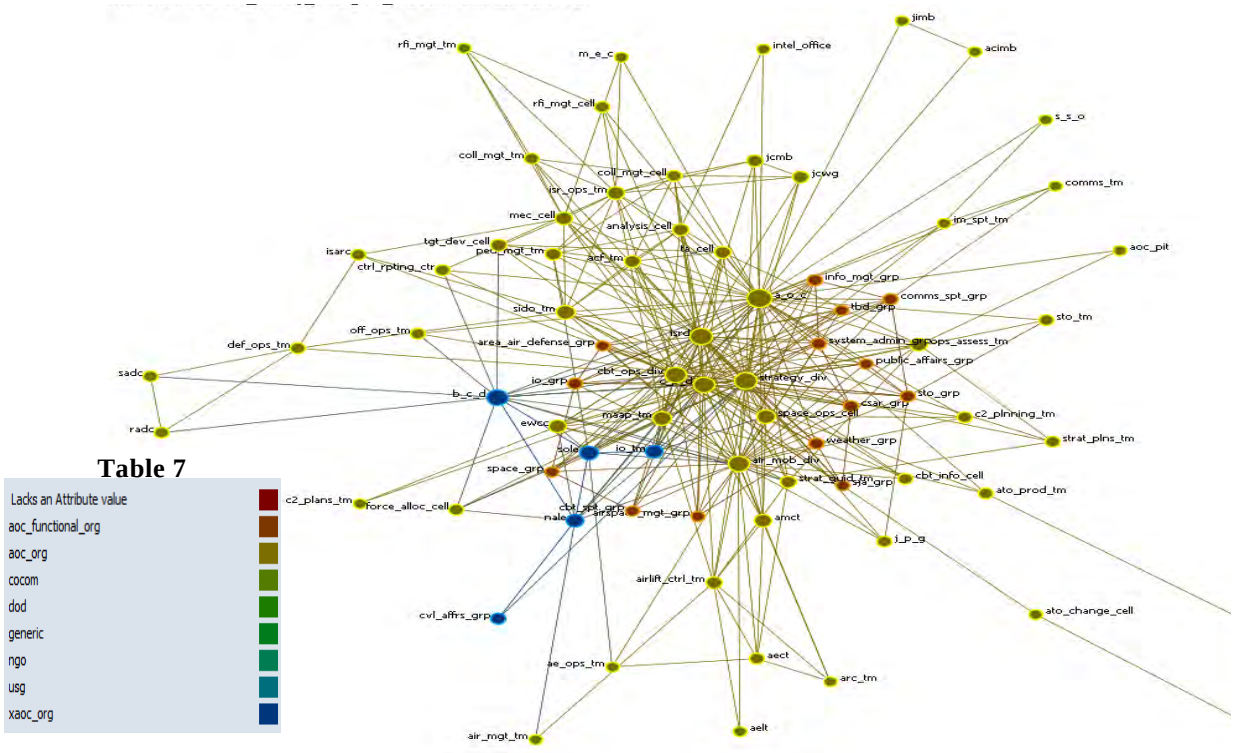

Figure 7 Agent x Agent Network of AOC divisions/teams/cells, AOC functional groups, and elements co-located with AOCs, sized by Centrality, Authority, colored by the 'category' of agent, removed isolates and pendants

2.3.2 ORA Analysis of Resilience for a Single Doctrine-based AOC

2.3.2.1 Network Descriptives

There were immediate and obvious advantages to the combining of the roles, organizations, and agents into a single node set and other data-to-model efforts. Though there were measures which had negative impacts, the balance tended to favor the extra data

Table 8 depicts two sets of information that are relevant to the resilience of a doctrinal-defined AOC. The first set of information, in column B, shows the benefits of performing additional data-to-model work in addition to text mining for each of the measures. Column C supports an assessment of organizational capabilities and resilience. Fundamentally, increasing the number of links between text-mined nodes allows us to more closely represent what an AOC member would call reality as well as improves values in 15 of 22 network measures (68.2% of the measures). The remainder of the table depicts the negative impacts to other network measures—illustrating tradeoffs inherent in model construction and modification.

Detailed descriptions of each measure are in (K. M. Carley et al., 2011), though a quick summary is appropriate. Table 8 tells us that there is better congruence between the knowledge agents need, given their assigned tasks than before the adjustments to the data. It also tells us that agents have less knowledge that is not used by their tasks than before the cleaning effort—the same is true of resource waste as well. The tasks that need resources also are better aligned with resources directly applicable to their tasks. The requirement to negotiate with other agents for knowledge and resources is lower, the number of resources and knowledge that are multi-

purposed has risen, task-related knowledge has risen, and the undersupply measures have both dropped..

In brief, the changes are leading to organizations that are more congruent and so more able to function in terms of people having the knowledge and resources needed for their tasks, less access to knowledge not need, and lots more communication than is strictly needed—which is a contributor to our later findings of high resilience.

2.3.3 Analysis of Key Entities Within ORA

To support an assessment of resilience, a first step is to identify which agents are important. ORA has a mechanism of performing this task through its *Key Entity Report*, agents listed in the Key Entity Report are consistently highly-ranked in various centrality and other measures ORA can calculate. An important feature of the *Key Entity Report* is that an analyst can, with high confidence, say which nodes are the top *n* most important. This is possible because the Key Entity reports calculates all available measures for the node sets and defined agents. ORA then creates a histogram of how often agents show up in the measures relevant to agents. Using this method, we identified the top 10 agents. We decided to perform multiple near term impacts analyses against the data set to determine if the removal of one of these top ten persons/roles or IT systems would negatively impact the performance metrics of the AOC. Though the degradation of operations through loss of personnel is beyond the scope of the paper's problem statement, it was a natural consequence of the merging of roles and organizations with the agent node set.

2.3.3.1 Central Roles and Agents

ORA is capable of generating 156 measures on meta-networks and nodes. The following are the results of the calculations of the key entity reports. The key entity report is a way of depicting more than the top set of nodes in any particular measure—instead it depicts the set of nodes that are the most frequently in the top set of nodes are across all applicable centrality measures for that node set. This allows us, with much higher confidence, report that a set of nodes in important to the entire meta-network. This confidence derives from the fact that the depicted node set is in the top 10 of many measures. The key entity report within ORA provided the top ten agents as shown below in Figure 8.

Table 8 Network-Level Measures for a doctrinal AOC, grey rows represent an improvement from Column A to Column C.

Network-Level Measure	Column A: Values from only source docs	Column B: Change	Column C: Source docs, figures, isolates reduced, binarized, symmetrized
Congruence, Communication	0.533	-176.41%	-0.407
Congruence, Org Agent Knowledge Needs	0.508	+68.23%	0.855
Congruence, Org Agent Knowledge Waste	0.059	-41.92%	0.034
Congruence, Org Agent Resource Needs	0.333	+ 142.11%	0.806
Congruence, Org Agent Resource Waste	0.126	-57.48%	0.053
Congruence, Org Task Knowledge Needs	0.132	-15.29%	0.112
Congruence, Org Task Knowledge Waste	0.382	+58.08%	0.604
Congruence, Org Task Resource Needs	0.090	+9.22%	0.098
Congruence, Org Task Resource Waste	0.348	+54.01%	0.536
Congruence, Social Technical	0.020	-13.33%	0.017
Congruence, Strict Knowledge	0.894	-12.52%	0.782
Congruence, Strict Resource	0.903	-11.12%	0.803
Negotiation, Knowledge	0.723	-6.50%	0.676
Negotiation, Resource	0.521	-18.08%	0.427
Omega, Knowledge	0.928	+4.10%	0.966
Omega, Resource	0.905	+5.85%	0.958
Performance As Accuracy	0.233	+31.79%	0.308
Task Completion, Knowledge Based	0.277	+ 17.00%	0.324
Task Completion, Overall	0.378	+ 18.70%	0.448
Task Completion, Resource Based	0.479	+ 19.68%	0.573
Under Supply, Knowledge	3.157	-28.92%	2.244
Under Supply, Resource	1.005	-29.55%	0.708

Figure 8 The top ten agents with a presence in the 23 relevant measures ORA calculates

The top ten agents are consistent within placing the responsibility for the AOC with combined/joint forces air component commander. Having the Chief of Combat Operations (CCO) Division as well as the Senior Operations Duty Officer (SODO) as essential figures is also consistent with the combat focus of the organization and the central role of the duty officer for each watch/shift. For aviators and aviation planning, Air Defense Artillery (ADA) is also important to planning and execution of offensive and defensive operations. All other agents are 10% or less of the measures. This can be taken as one sign that the function and operation of the AOC is not overly dependent on any single person, though a combination of four individuals clearly dominate the various measures.

2.3.3.2 Central Organizations

For the agents listed in Figure 9, all five AOC divisions are prominent and taken together dominate the organization. The doctrine authors certainly convey the importance of thorough planning and the essential nature of the sustaining logistics base for modern warfare through the dominance of the Strategy Division and the Air Mobility Division. The modern Air Force's dependence of space-based assets is also represented as is the Master Air Attack Plan (MAAP) team.

Figure 9 The top ten organizations with a presence in the 19 relevant measures ORA calculates

2.3.3.3 Central Information Technology (IT) Systems

With the concern about the ability to operate in a degraded cyber environment is it now appropriate to see which of the various IT systems and resources documented in the doctrine are in the Key Entity Report. From the chart below, as well as discussions with a former CJFACC, the Theater Battle Management Core System (tbmcs below) is indeed a key and essential system the AOC uses. The underlying communications infrastructure (comms and comms_sys) is also in over 50% of the measures though it remains frustratingly vague to those tasked with defending cyberspace resource—it's akin to saying 'defend everything,' which Soldiers almost universally understand as 'defend nothing well.' With the presence of the Command and Control Personal Computer (C2PC), the Global Command and Control System (GCCS), these became prime candidates for performing an immediate impact report and near term analysis. Based on discussions with the former Numbered Air Force (NAF) Commander, we also included the Joint Automated Deep Operations Coordination System (JADOCS).

With the information in Figure 10, we begin to have an analytic basis for assessing that there may be systems without which AOC operations will be significantly impacted. With the intuition that a system that is in the top 10 of 60% of relevant measures (i.e. TBMCS) and top 25% (e.g. C2PC, GCCS), we can transition over to an immediate impact report and near term analysis that focuses on the IT systems of the AOC rather than specific individuals, roles, or sub-organizations.

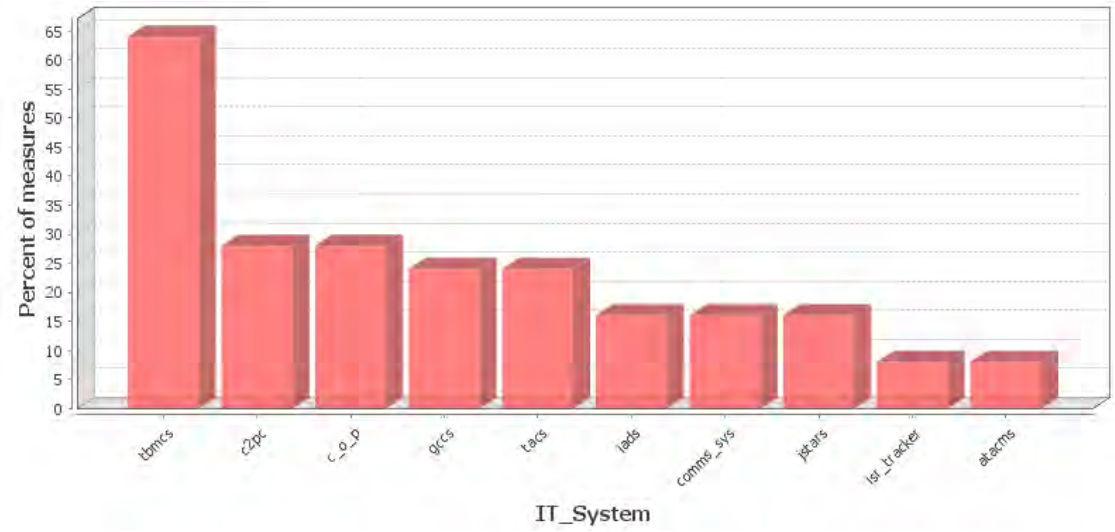

Figure 10 The top ten IT systems/resources with a presence in the 19 relevant measures ORA calculates

2.3.4 Immediate Impact Reporting

The static analysis above is a robust way of measuring nodes' importance to the whole network across many different measures. However, many organizations only truly acknowledge the importance of a person/resource/knowledge when they no longer have access to that person/resource/knowledge. To simulate this loss, we conduct two types of impact analysis, both supported by ORA: Immediate Impact Report and Near Term Analysis.

The immediate impact analysis report calculates the change in network level measures, cognitive demand, degree centrality, and betweenness centrality immediately following a node removal. We can accomplish node removal in one of two ways: random removal over *x* replications or specified node removal. We used this data to assess whether removing a random node(s) or a key actor(s) had an impact on the network. The Near Term Analysis allows us, within ORA, to perform a micro-simulation using another tool provided by CASOS: Construct. The Near Term Analysis helps identify how a network will adjust over the course of time after removal of a node.

2.3.4.1 Immediate Impact Metrics

Network Level Metrics: The specific metrics included in the Network Level Metrics category are: number of nodes, overall complexity, performance as accuracy, diffusion, clustering coefficient, characteristic path length, social density, communication congruence, average communication speed, number of isolated agents, fragmentation, overall fragmentation. These metrics provide information regarding how the network operates as a whole and have extensive explanations to their derivations in the ORA User's Guide (K. M. Carley, Columbus, DeReno, et al., 2011).

Cognitive Demand: It takes cognitive effort to engage with external entities, so knowing how much effort nodes expend can provide useful information. Nodes high in cognitive demand are likely connected to many people, organizations, tasks, events, areas of expertise, and resources. Those same nodes are also more engaged in complex tasks where they may not have all the needed resources or knowledge—this deficit will require nodes to coordinate with other nodes to gain access to needed resources and knowledge. These nodes are often considered emergent leaders because of their high level of activity in the network.

Degree Centrality: The Degree Centrality of a node is the sum of its row and column degrees normalized to a scale between 0 and 1. Nodes with high degree centrality have links to many others and have access to the ideas, thoughts, and beliefs of many other nodes. These nodes are often hubs of information because of their extensive connections in the network.

Betweenness Centrality: Betweenness centrality represents the level of connectedness to other parts of the network. Betweenness is measured by the count of times a node is present on the paths between any two nodes in the network. These nodes are often facilitators of communication because they act as a bridge between other nodes.

2.3.4.2 'Suggestive' and 'Meaningful' Impacts of deleting single IT systems

In our analysis, we label as "suggestive" percentage changes greater than or equal to approximately 5%. We give the label "meaningful" to any changes greater than or equal to 10%. We do not attempt to assert statistical significance to the changes, because, as noted before, we do not know the underlying probability distribution.

2.3.4.3 Random Deletion

For this analysis, the authors used ORA's Immediate Impact Report on both the completely merged input file (where all agent-like entities where in the agent class) (see also Figure 12) as well as the partially merged input file (where IT-systems/resource where in their own node class). We had ORA randomly delete four (4) nodes and ran 100 replications. ORA then presented the average changes to the thirty-seven measures the immediate impact report generates. Only one measure rose above the 'suggestive' threshold of 5% ().

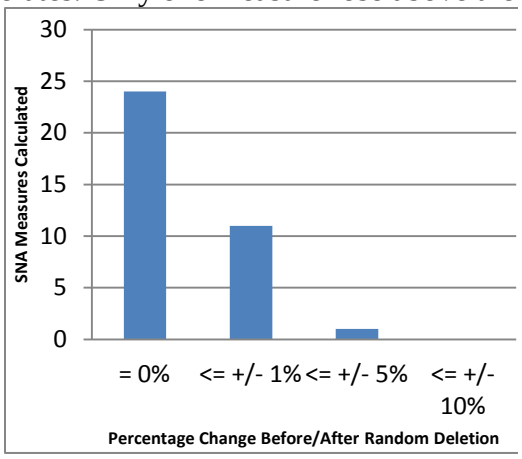

Figure 11 Effects for Random Deletion/Targeting of IT-Systems

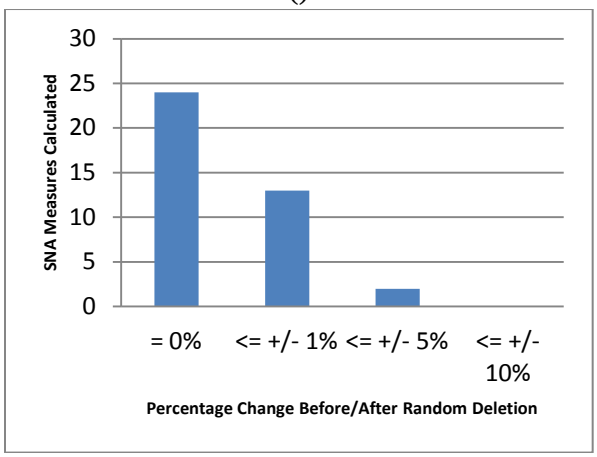

Figure 12 Effects for Random Deletion/Targeting of combined agent node class

This result was not surprising as the distribution of the total links per node (Centrality Degree) is nearly a logarithmic decay—there is a lower probability that random selection of four nodes will end up with high-centrality nodes. The figures below show the degree distribution of both the completely merged input file (Figure 13) as well as the file with IT systems/resources separated from other kinds of agents (Figure 14).

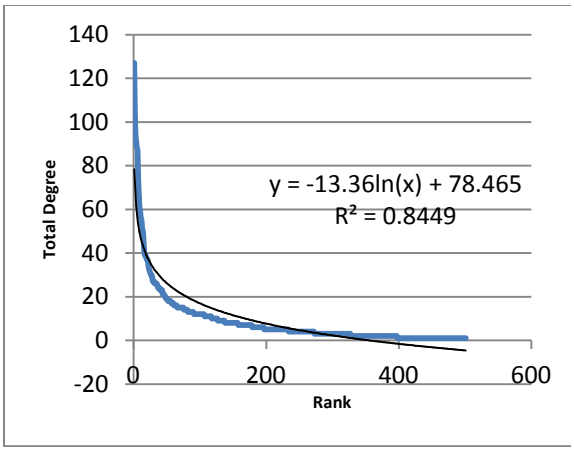

Figure 13 Total Degree Distribution, All Agents

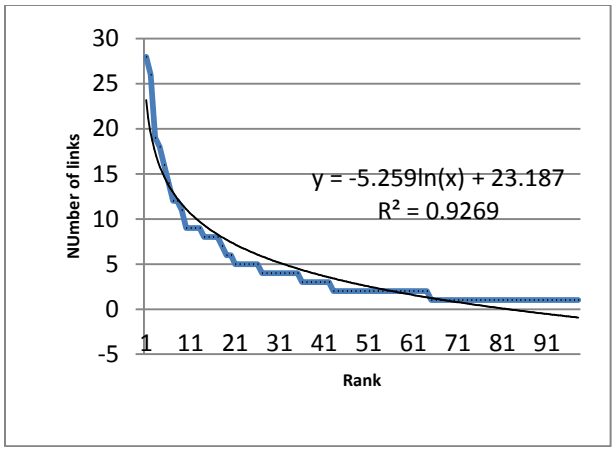

Figure 14 Total Degree Distribution - IT-Systems Only

This low probability of randomly deleting a critical node, and more importantly a group of critical nodes, drove the researchers to use the targeted node removal instead. Targeted node removal in the context of this project is the equivalent of a 100% denial of availability—it could be physical destruction or total system isolation. The next section reviews the impacts of removal in singular actions as well as some combinations of isolations.

2.3.4.4 Targeted Deletion

2.3.4.4.1 Threat Battle Management Core System (TBMCS)

There were no suggestive or meaningful changes to network level measures when IT Systems remained in the agent node class. When segregated into their own node class, the following table resulted.

Network Level Measures (for IT Systems only)

Name	Before	After	Percent Change
Performance As Accuracy	0.045	0.028	-38.77%
Clustering coefficient	0.275	0.250	-9.10%
Characteristic Path Length	2.956	3.415	+ 15.53%
Social Density	0.021	0.018	-12.63%
Communication Congruence	-0.490	-0.556	+ 13.53%

Cognitive Demand had no suggestive or meaningful changes.

There were no suggestive or meaningful changes to Centrality (total degree) when IT Systems remained in the agent node class. When segregated into their own node class, the following table resulted.

Centrality (total degree centrality) (for IT Systems only)

Name	Before	After	Percent Change	Name	Before
tbmcs	1	0.207	Entity removed		
gdss	6	0.097	5	0.090	-6.50%
g_t_n	7	0.090	6	0.083	-7.05%
trac2es	8	0.090	8	0.083	-7.05%
jwics	10	0.069	10	0.063	-9.38%

Betweenness Centrality (for combined agent node class)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
air_mob_div	2	0.088	2	0.093	6.36%
tbmcs	1	0.088	Entity removed		
gccs	5	0.029	3	0.052	+77.72%
strategy_div	7	0.041	7	0.043	5.82%
c2pc	8	0.034	6	0.045	32.23%
c_c_o	9	0.029	8	0.034	17.27%
sodo	10	0.026	10	0.027	6.93%

Betweenness Centrality (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	1	0.088	Entity removed		
c2pc	2	0.069	1	0.103	+48.87%
gccs	5	0.029	3	0.052	+77.72%

The TBMCS is a web-enabled database accessible to all members of the AOC that supports management of combat operations. AOC members use it to communicate information throughout the AOC and ensure that all members are up-to-date on current operations.

The lack of changes suggestive or meaningful changes when there is a single agent node class indicates that, in this instance, the remaining nodes' influence are driving the overall network performance. When we isolated the IT Systems from the other agents, the network level measures tell us that if some event (cyber or otherwise) removed TBMCS from service, the performance as accuracy drops—congruent with the intuitive expectation after seeing its position in the IT System Key Entity chart (see Figure 10). Communication congruence has risen as agents will have less access to knowledge not needed to execute their assigned tasks. Centrality effects are congruent with TBMCS being so well connected within the network. It is not surprising that C2PC and GCCS become the new go-to IT systems, though the emergence of the Portable Flight Planning System (PFPS) was not expected given its absence from the Key Entity report. The nodes that gain betweenness centrality are used in place of the tbmcs to connect to other nodes.

The rise in betweenness centrality (being on the most shortest paths between any two agents) for the Chief of Combat Operations(c_c_o) and the Senior Operations Duty Officer (sodo) are indicative of the current USAF technique of using humans to overcome shortfalls in IT systems' performance.

2.3.4.4.2 Global Command and Control System (GCCS)

There were no suggestive or meaningful changes to any of the measures when IT Systems remained in the agent node class. When segregated into their own node class, the following tables resulted.

Network Level Measures (for IT Systems only)

Name	Before	After	Percent Change
Clustering coefficient	0.275	0.257	-6.51%
Social Density	0.021	0.019	-7.49%

Cognitive Demand had no suggestive or meaningful changes.

Centrality (total degree centrality) (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
pfps	5	0.110	4	0.104	-5.60%
gdss	6	0.097	5	0.090	-6.50%
g_t_n	7	0.090	6	0.083	-7.05%
trac2es	8	0.090	7	0.083	-7.05%
gates	9	0.083	8	0.076	-7.70%
jwics	10	0.069	9	0.069	+0.69%

Betweenness Centrality (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	1	0.112	1	0.126	+ 12.83
c2pc	2	0.069	1	0.080	+ 16.55%
gccs	5	0.029	Entity Removed		

GCCS is an IT system that comes in a variety of flavors and end-user systems. It is a collection of service oriented architecture (SOA) data consumers and data producers that have a common of flattening the information diffusion hierarchy within the DoD.

From the network level metrics, GCCS is not as tied into other IT systems (or human agents) as the acquisition program would desire. Referring back to Figure 10, GCCS is not as prominent or dominant as TBMCS, making no discernable impact on performance as accuracy or congruence measures. The drop in centrality for five (5) of ten (10) systems reflects their being connected to the well-connected GCCS. The change in JWICS (Joint Worldwide Intelligence Communications System) is unusual, as GCCS is usually on unclassified and secret computer networks, not top secret computer networks.

2.3.4.4.3 Command and Control Personal Computer (C2PC)

Network Level Measures (for combined agent node class)

Name	Before	After	Percent Change
Number of Isolated Agents	85	90	5.88%
Overall Fragmentation	0.004	0.007	74.95%

Network Level Measures (for IT Systems only)

Name	Before	After	Percent Change
Performance As Accuracy	0.044	0.049	+ 11.69%
Diffusion	0.275	0.251	-8.88%
Clustering Coefficient	0.275	0.254	-7.52%
Social Density	0.021	0.018	-11.23%

Cognitive Demand had no suggestive or meaningful changes.

There were no suggestive or meaningful changes to Centrality (total degree) when IT Systems remained in the agent node class. When segregated into their own node class, the following tables resulted.

Centrality (total degree centrality) (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
pfps	5	0.110	4	0.104	-5.60%
gdss	6	0.097	5	0.090	-6.50%
g_t_n	7	0.090	6	0.083	-7.05%
trac2es	8	0.090	7	0.083	-7.05%
gates	9	0.083	8	0.076	-7.70%

Betweenness Centrality (for combined agent node class)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	3	0.067	3	0.07	5.06%
c_c_o	9	0.029	10	0.025	-11.95%

Betweenness Centrality (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	1	0.112	1	0.124	+ 10.37%
gccs	5	0.029	2	0.044	+50.77%
pfps	10	0.019	7	0.023	+ 17.70%

C2PC is a Microsoft Windows™-based application that can share and edit a GCCS common operating picture (COP). Additionally, users can add and apply operational graphics, display imagery from

various sources, and send/receive messages (akin to instant messaging) to other C2PC systems/users.

With the loss of C2PC, (second most prominent system in Figure 10), there is suggestive rise in the number of isolated agents and a pronounced change in the fragmentation of the overall network. This indicates that C2PC is serving as a bridging role in multiple places in the network, and AOC personnel will feel its loss.

Performance as Accuracy, unintuitively, rises as a result of a decrease in the number of systems users can access, and potentially get erroneous information from. Unfortunately, it coincides with a slowdown in the diffusion of information as well as a decrease in the clustering coefficient and social density.

The decrease in connectivity for five (5) of the top ten (10) IT systems is consistent with deletion of a well connected node. The rise in betweenness centrality for TBMCS and GCCS was not surprising though the concurrent rise in the portable flight planning system (pfps) was not expected. Additionally the drop in betweenness centrality for the Chief of Combat Operations was surprising.

2.3.4.4.4 Joint Automated Deep Operations Coordination System (JADOCS)

Network Level Measures had no suggestive or meaningful changes.

Cognitive Demand had no suggestive or meaningful changes.

There were no suggestive or meaningful changes to Centrality (total degree) when IT Systems remained in the agent node class. When segregated into their own node class, the following tables resulted.

Centrality (total degree centrality) (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
pfps	5	0.110	4	0.104	-5.60%
gdss	6	0.097	5	0.090	-6.50%
g_t_n	7	0.090	6	0.083	-7.05%
trac2es	8	0.090	7	0.083	-7.05%
gates	9	0.083	8	0.076	-7.70%

Betweenness Centrality (for combined agent node class)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
c2pc	8	0.034	8	0.038	+ 11.76%

Betweenness Centrality (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
c2pc	2	0.069	2	0.076	+ 10.53%

JADOCS is mission management software that integrates with TBMCS at the wing and squadron levels of operations. It helps build the counter fire common operating picture (CF-COP) and other fire support/planning functions. JADOCS was not in Figure 10, though we included it in the list of systems for assessment as the recommendation of a former C/CJFACC.

The decrease in connectivity for five (5) of the top ten (10) IT systems is consistent with deletion of a semi-well connected node. The rise in betweenness centrality for C2PC reflects the use of that system in interface with TBMCS and GCCS.

The lack of suggestive or meaningful effects is likely a reflection on the relative lack of emphasis on JADOCS in the source documents.

2.3.4.5 Impacts of simultaneously deleting/targeting multiple IT systems

2.3.4.5.1 TBMCS & GCCS

There were no suggestive or meaningful changes to Network Level Measures when IT Systems remained in the agent node class. However, eight(8) of the eleven(11) measures did have non-linear effects—possibly revealing an interaction effect that AOC system and process designers were unaware of. When we segregated IT Systems into their own node class, the following tables resulted.

Network Level Measures (for IT Systems only)

Name	Before	After	Percent Change
Performance As Accuracy	0.045	0.030	-33.54%
Diffusion	0.275	0.221	-19.64%
Clustering Coefficient	0.275	0.238	-13.25%
Characteristic Path Length	2.956	3.336	+ 12.86%
Social Density	0.021	0.016	-19.93%
Communication Congruence	-0.490	-0.569	+ 16.19%
Average Communication Speed	0.338	0.300	-11.39%
Fragmentation	0.721	0.775	+7.51%

Cognitive Demand had no suggestive or meaningful changes.

There were no suggestive or meaningful changes to Centrality (total degree) when IT Systems remained in the agent node class. When segregated into their own node class, the following table resulted.

Centrality (total degree centrality) (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	1	0.207	Entity removed		
c2pc	2	0.186	1	0.175	-6.11%
Gccs	3	0.131	Entity removed		
jadocs	4	0.124	2	0.112	-9.87%
gdss	6	0.097	4	0.084	-13.09%
g_t_n	7	0.090	5	0.077	-14.20%
trac2es	8	0.090	7	0.077	-14.20%
gates	9	0.083	6	0.077	-7.05%
jwics	10	0.069	8	0.063	-8.74%

Betweenness Centrality (for combined agent node class)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
air_mob_div	2	0.088	2	0.093	6.54%
isrd	4	0.058	3	0.061	5.35%
strategy_div	7	0.041	7	0.043	5.61%
c2pc	8	0.034	5	0.046	36.65%
c_c_o	9	0.029	8	0.03	5.76%
sodo	10	0.026	9	0.028	7.66%

The dominant change illustrated above is the meaningful rise in the betweenness centrality of c2pc followed in the distance by the other agents listed. The three divisions, as organization nodes, rose in importance, as did the Chief of Combat Operations and the Senior Operations Duty Office.

Betweenness Centrality (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	1	0.112	Entity removed		
c2pc	2	0.069	1	0.106	+53.15%
tacs	3	0.041	4	0.037	-10.24%
adsi	4	0.034	6	0.030	-10.27%
gccs	5	0.029	Entity removed		
stars	8	0.021	10	0.019	-9.74%
jwics	9	0.020	3	0.043	+ 114.78%
pfps	10	0.019	7	0.022	+ 13.04%

The combined loss of TBMCS and GCCS has a larger effect on the AOCs' IT Systems' distribution of knowledge than the loss of either of them in isolation as well as their summed losses—there is an interaction effect between the loss of both these systems across every agent in the report.

2.3.4.6 GCCS and C2PC

The effects of the loss of all the GCCS and C2PC IT systems are non-linear in eight (8) of the eleven (11) measures. There is also a larger percentage effect when we isolate the IT systems from the other types of agents in the node class as these next two tables illustrate.

Network Level Measures (for combined agent node class)

Name	Before	After	Percent Change
Number of Isolated Agents	85	97	14.12%
Overall Fragmentation	0.004	0.007	75.04%

Network Level Measures (for IT Systems only)

Name	Before	After	Percent Change
Performance As Accuracy	0.041	0.044	+7.76%
Diffusion	0.225	0.199	-11.59%
Clustering Coefficient	0.261	0.223	-14.69%
Characteristic Path Length	2.853	3.096	+8.49%
Average Communication Speed	0.350	0.323	-7.83%
Overall Fragmentation	0.004	0.007	+75.04%

Cognitive Demand had no suggestive or meaningful changes.

There were no suggestive or meaningful changes to Centrality (total degree) when IT Systems remained in the agent node class. When segregated into their own node class, the following tables resulted.

Centrality (total degree centrality) (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	1	0.194	1	0.183	-5.84%
jadocs	4	0.125	2	0.113	-9.86%
pfps	5	0.111	3	0.099	-11.27%
gdss	6	0.097	4	0.085	-13.08%
g_t_n	7	0.083	5	0.070	-15.49%
trac2es	8	0.083	6	0.070	-15.49%
gates	9	0.076	7	0.063	-17.03%

Betweenness Centrality (for combined agent node class)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
c_c_o	9	0.029	9	0.024	-16.87%

Betweenness Centrality (for IT Systems Only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	1	0.080	1	0.111	+39.51%
tacs	3	0.037	4	0.035	-5.34%
jadocs	7	0.018	3	0.036	+98.49%
pfps	8	0.018	4	0.030	+68.03%
i_w_s	i_w_s	9	0.017	10	0.014

Again there are mixed messages in these results. When these two systems are not mission capable, the Chief of Combat Operations declines in betweenness centrality, but there were no other centrality affects rising above the 5% change threshold for being suggestive when measuring across the entire AOC, its personnel, knowledge, sub-organizations, etc. When we constrain analysis to IT systems, the impact becomes more apparent. In particular there was a sudden shift tbmcs, jadocs, and the portable flight planning system (pfps).

2.3.4.6.1 C2PC and JADOCS

The effects of the loss of all the C2PC and JADOCS IT systems are non-linear in one (10) of the eleven (11) measures. There is also a larger percentage effect when we isolate the IT systems from the other types of agents in the node class as these next two tables illustrate.

Network Level Measures (for combined agent node class)

Name	Before	After	Percent Change
Number of Isolates	85.000	91.000	+7.06%
Overall Fragmentation	0.004	0.007	+75.04%

Network Level Measures (for IT Systems only)

Name	Before	After	Percent Change
Diffusion	0.225	0.199	-11.55%
Clustering Coefficient	0.261	0.239	-8.47%
Characteristic Path Length	2.853	3.030	+6.20%
Social Density	0.020	0.016	-18.85%

Cognitive Demand had no suggestive or meaningful changes.

Centrality (total degree) had no suggestive or meaningful changes for the combined agent node class. When we restrict the analysis to only the IT-systems view, the following table results.

Betweenness Centrality (for IT Systems Only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	1	0.194	1	0.183	-5.84%
gccs	3	0.132	2	0.120	-9.27%
pfps	5	0.111	3	0.099	-11.27%
gdss	6	0.097	4	0.085	-13.08%
g_t_n	7	0.083	5	0.070	-15.49%
trac2es	8	0.083	6	0.070	-15.49%
gates	9	0.076	7	0.063	-17.03%
jopes	10	0.063	9	0.056	-9.86%

Betweenness Centrality (for combined agent node class)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	3	0.067	3	0.078	+ 16.91%
c_c_o	9	0.029	10	0.025	-13.12%
sodo	10	0.026	8	0.027	+5.85%

Betweenness Centrality (for IT Systems Only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tbmcs	1	0.080	1	0.107	+34.91%
tacs	3	0.037	3	0.035	-5.34%
adsi	4	0.030	4	0.027	-8.20%
gccs	5	0.028	2	0.044	+59.95%
pfps	8	0.018	6	0.021	+ 19.21%
i_w_s	9	0.017	11	0.012	-26.15%

Again there are mixed messages in these results. When these two systems are not mission capable, tbmc rises in betweenness centrality as does the Senior Operations Duty Office (SODO), while the Chief of Combat Operations declines. When we constrain analysis to IT systems, the impacts become more apparent. In particular rise in importance of GCCS and PFPS as fast ways to pass information between any two agents.

2.3.4.6.2 TBMCS, GCCS, C2PC, and JADOCS

The effects of the loss of all four IT systems are non-linear in ten (10) of the eleven (11) measures. There is also a larger percentage effect when we isolate the IT systems from the other types of agents in the node class as these next two tables illustrate.

Network Level Measures (for combined agent node class)

Name	Before	After	Percent Change
Performance As Accuracy	0.299	0.283	-5.44%
Diffusion	0.62	0.571	-8.03%
Clustering Coefficient	0.377	0.349	-7.42%
Social Density	0.013	0.012	-6.30%
Number of Isolated Agents	85	97	14.12%
Fragmentation	0.377	0.427	13.22%
Overall Fragmentation	0.004	0.007	75.22%

Network Level Measures (for IT Systems only)

Name	Before	After	Percent Change
Performance As Accuracy	0.043	0.025	-42.08%
Diffusion	0.225	0.130	-42.01%
Clustering Coefficient	0.261	0.173	-33.71%
Characteristic Path Length	2.853	4.380	+53.48%
Social Density	0.020	0.012	-38.30%
Communication Congruence	-0.465	-0.547	+ 17.63%
Average Communication Speed	0.350	0.228	-34.85%
Fragmentation	0.773	0.867	+ 13.22%
Overall Fragmentation	0.004	0.007	+75.22%

At the meta-network level, across all agents, resources, tasks, and other nodes in the model, the overall impact is not as great as our intuition indicated. This can be an indication of the resilience of the AOC and its ability to conduct *mission assurance* in the face of cyber attacks. A note of caution is important however that when reviewing the static analysis of just IT systems, the *performance as accuracy, diffusion, communication speed* are all impacted more than measures across the whole network would indicate. These measures' impacts are reflective of the current fears of cyberspace attacks at the same time that entire network measures indicate the fears may be overblown.

Cognitive Demand had no suggestive or meaningful changes.

There were no suggestive or meaningful changes to Centrality (total degree) when IT Systems remained in the agent node class. When segregated into their own node class, the following tables resulted.

Centrality (total degree centrality) (for IT Systems only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
pfps	5	0.111	1	0.093	-16.43%
gdss	6	0.097	2	0.071	-26.53%
g_t_n	7	0.083	3	0.057	-31.43%
trac2es	8	0.083	6	0.057	-31.43%
gates	9	0.076	4	0.057	-25.19%
jopes	10	0.063	7	0.050	-20.00%

Betweenness Centrality (for combined agent node class)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
c_c_o	9	0.029	9	0.024	-16.62%
sodo	10	0.026	8	0.031	20.53%

Betweenness Centrality (for IT Systems Only)

Name	Rank Before	Value Before	Rank After	Value After	Value Change (%)
tacs	3	0.037	6	0.028	-24.50%
adsi	4	0.030	10	0.019	-34.25%
stars	6	0.019	11	0.015	-23.19%
pfps	8	0.018	4	0.030	+68.03%
i_w_s	9	0.017	5	0.028	+65.84%
jwics	10	0.016	1	0.071	+331.99%

Again there are mixed messages in these results. When these four systems are not mission capable, the SODO will rise in importance while the Chief of Combat Operations declines, but there were no other centrality affects rising above the 5% change threshold for being suggestive when measuring across the entire AOC, its personnel, knowledge, sub-organizations, etc. Only when we constrain analysis to IT systems does the impacts become more apparent. In particular, there is a sudden shift to TS/SCI networks (jwics) and its messaging and collaboration application (iws).

2.3.5 Immediate Impact Reports Conclusions

Analysis of this model and this extreme case, a total denial of availability of four (4) key IT systems, in the context of the entire AOC, revealing a surprising but reassuring result: there are no catastrophic consequences predicted. This must be taken with a grain of salt however. The result is a snap shot in time, not a prediction over time. Equally important, the assessment assumes perfect assumption of communications by remaining IT systems and perfect adaptation by humans—neither of which is feasible without excellent continuity of operations plans and rehearsals of those plans.

When assessed exclusively in an IT-System ecosystem context, there are many SNA measures that are well past the 'suggestive' and 'meaningful' thresholds, some approaching a 50% drop in values from uncontested to contested environments. This is consistent with the perception of technologists that the AOC is extremely vulnerable to cyber attacks. Clearly, a contested cyber environment will affect elements of the AOC differently. The most important lesson of this section is there is analytic support for Airmen who argue that 'the war will go in' even if the 'network is down.'

2.3.6 Near Term Analysis and Conclusions

ORA has an additional way of assessing the impacts of various changes to a network. A researcher accesses this method through the Simulations Menu of ORA, and selecting the Near Term Analysis (NTA) option.

The NTA is a simplified interface and means of accessing the agent-based model (ABM) application, Construct. A more thorough discussion of Construct is in the next chapter. Within NTA, agents interact with each other, exchanging knowledge, for one of two principal reasons: homophily (e.g., similarity as inferred from agents' perception of their own knowledge and their perception of others' knowledge) and expertise seeking (e.g., seeking knowledge an agent does not have). NTA requires a meta-network to have, minimally, the following node sets: agents, tasks, and knowledge. The simulation supports and uses a belief node set as well, though the node set is not mandatory.

When using NTA, a researcher has the option of exploring the impacts of various actions. Actions can include isolating/deleting of one or more agents, knowledge, tasks, and beliefs at the same or various times during the simulation. Another action could include adding knowledge (e.g., an intelligence report). Nodes can be isolated by directed specific targeting as well as through the use of ORA-calculated measures (i.e., Centrality, Total Degree; Cognitive Demand; Clique Count; Centrality, Betweenness; Exclusivity, Task; Exclusivity, Knowledge). In addition to using those measures, the researcher can set a specified isolation time as well as a specified number of nodes to isolate. The nodes a researcher can isolate are Agents, Knowledge, and Resources.

The figure below depicts the impact of single-node isolation at time zero (0) of each of the top nodes we deleted in the static analysis. The figure depicts the overall change in knowledge diffusion from the baseline. We set NTA to run for 25 time periods, meaning each agent has 25 opportunities to interact with other agents. The primary measure of interest for NTA is knowledge diffusion, simulated through the injection of a single bit of knowledge to a random location and determining how well knowledge of that bit extends throughout agent network.

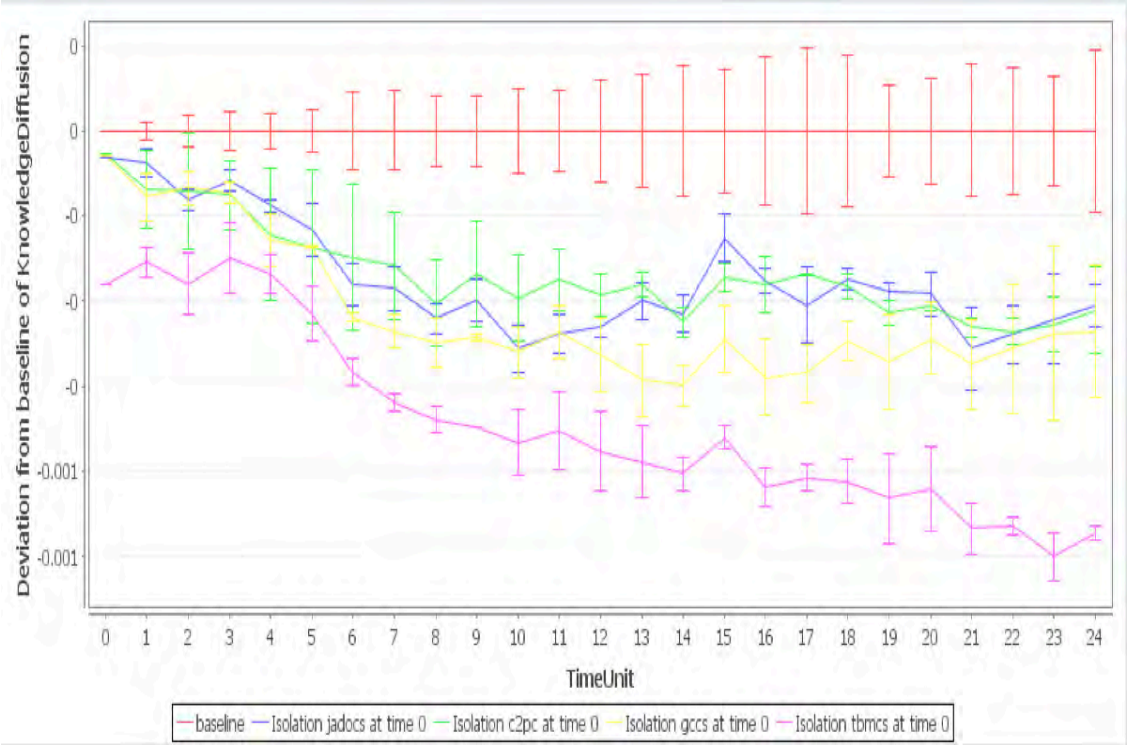

Figure 15 Change in Diffusion of Knowledge over Time from ORA's Near Term Analysis

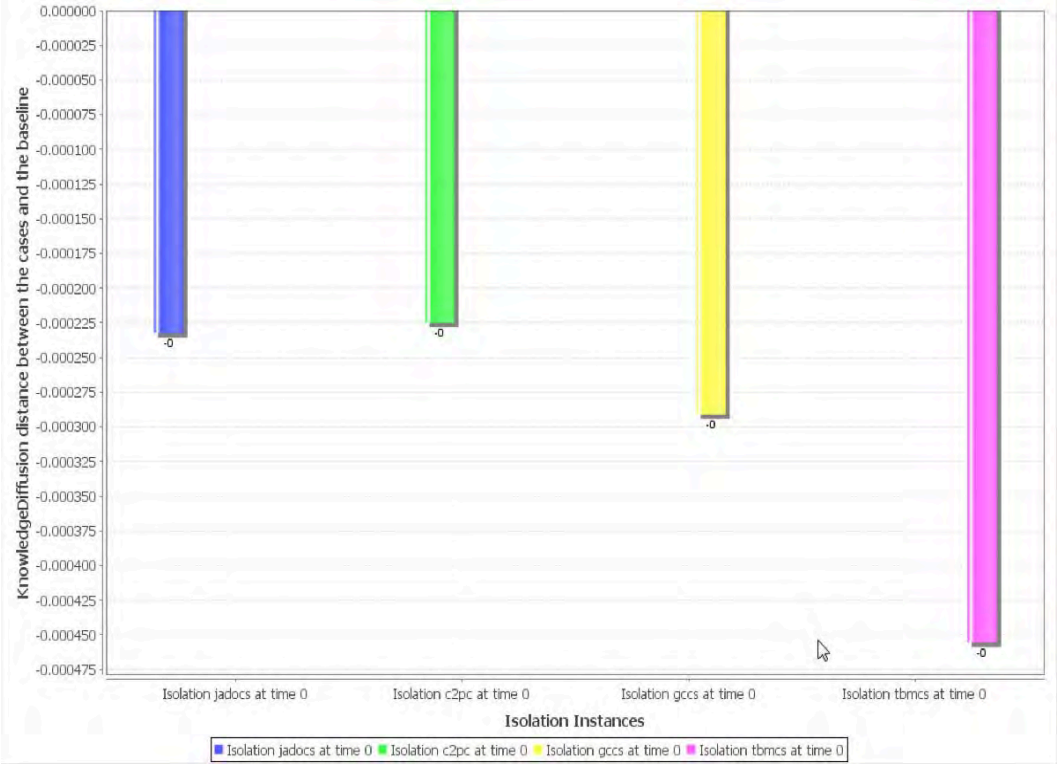

Figure 16 Change in Diffusion of Knowledge, at time period 25 of 25, for deletion of single agents at time 0

When we use the Near Term Analysis capability to assess degradation of combinations of two IT System the degradation is non-linear, as it was in the static analysis.

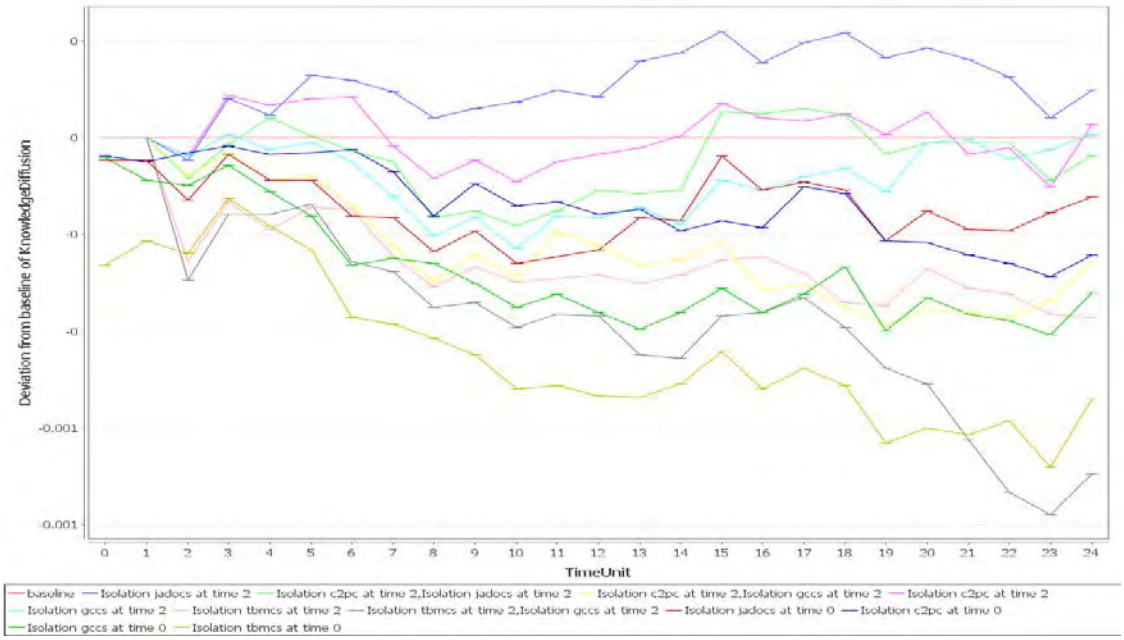

Figure 17 Change in Diffusion of Knowledge over Time from ORA's NTA, using combinations of IT-Systems

Each of these charts (Figure 15, Figure 16 and Figure 17) represent the change in knowledge diffusion normalized between -1 to 1, by dividing the total number of agents with the inserted knowledge by the total number of agents. Depending on the size of the network under review, NTA may be sufficient to identify answers to questions-of-interest. For the resilient C2 project, NTA results are illustrative, congruent with the static analysis, and provoke the realization that 25 turns for a multi-thousand agent network is probably insufficient time to have confidence that the result(s) hold true over time. To raise the confidence level, we will turn to the non-ORA interface of Construct in the next chapter.

2.4 Discussion and Contributions for SNA Analysis of Resilience

2.4.1 The Challenges of Doctrine with Text Mining

Text mining from different domains of human knowledge can present distinctly domain dependent challenges. US DoD doctrine, both Service and Joint, is replete with exemplars of some of the toughest challenges in the Natural Language Processing (NLP) research arenas. To borrow a phrase, doctrinal language is not natural language.

This effort used only four documents, for an approximate combined length of 2,800 pages of primary text, diagrams, tables, references, and appendices. Incorporating additional references that may not be directly applicable to the AOC, but have direct bearing on the missions they support (e.g., strategic logistics, close air support, strategic air refueling, and air superiority) would likely expand the reaches of the overall network. While this could be problematic from the organizational viewpoint (those other documents will surely include non-AOC organizations) it would likely increase the overall density of the network through the explicit discussion of concepts that USAF writers take for granted—in other words, increased heterogeneity of authors will likely make for a more complete model, as they do not share the same assumptions and views about what they are writing.

Along with additional DoD doctrinal references, it would be potentially useful to vary the values used by researchers in the data-to-model process. While it is unlikely that an exhaustive exploration of all input values is necessary, it is probable that a range(s) of inputs (e.g., window size, stop-unit select and stop-unit-counter limits, thesaurus) of selections produce the most consistent models as measured by the deviations of their network and select entity-level measures. By having a larger set of networks drawn from the same data sources, it is feasible that we could determine statistical significance to the changes in the output variables.

2.4.2 Military Command Hierarchies and Matrix Support

We saw from the network model derived from text-mining doctrinal references that dominate nodes (in entity level measures, network level measures, and in impact reports) were generally not the heads of five (5) doctrinal divisions, nor even the director of the AOC. While this information is insufficient to gauge absolute relevance, it should serve as a reminder to organizational designers and force planners that the force of personality may be important, but it cannot be the basis of organizational performance or continuity. Indeed, the model suggests that the more doctrinal references address non-strict hierarchal interactions between organizations and people, the more likely the organization is to be resilient to a contest cyber environment—the quantity of links between people, organizations, roles, knowledge, tasks, and resources will tend to mitigate against the loss of links between IT-Systems and between humans and IT-Systems. This provides analytic support to the decision by the USAF to provide resilience to a contest cyber environment through the use of humans.

The matrix support enumerated in the source documents, as well as depicted in Figure 2, is a contested-cyber environment mitigation—though not intended as such. What started as a realization that no finite hierarchy can cleanly divide all tasks among its branches, has lead to a hybrid of hierarchy and functional group organization. This hybridization clearly has benefits in supporting leaders' task delegation and matching expertise to tasks. Additionally, the hybridization increases the formal and informal links between people, roles, and organizations. With increased links, comes increased probabilities of interaction, information sharing, sharing a common culture and situation understanding, ultimately leading to organizational effectiveness. These additional links make the network resistant to catastrophic damage from random failures and attacks. The extra links also decrease the prominence of any particular agent, role, IT-System, and organization—further militating against loss of any single node in the overall network.

There is clearly trade space between additional links (compared to a strict hierarchy or strict matrix organization) and an excessive number of links that lead to inefficiencies. Those inefficiencies are measurable in this kind of model—and models that replicate burdensome staffing and routing procedures would reflect the inefficiencies even more prominently. Inefficiencies are the bedfellow of resilience—a 100% efficient organization, with no mismatch between that which it needs and that which it has, that which it does and that which it needs to do, is an organization that has little to no resilience in the face of non-optimal conditions.

2.5 Future Work in SNA and Modeling Through Text Mining

2.5.1 Results-suggested Areas for Further Refinement and Work

The immediate impact analysis report on agents and roles (e.g., total removal from the network) is not generally representative of a situation that would actually occur. While clearly loss of individuals occurs, one of the on-going tasks in every military organization is the training

of subordinates and peers to assume the duties of fallen leaders. The over-time execution of this task, as well as the near-continuous personnel turbulence of military organization is not well reflected in the model but does serve to reduce the probability that tacit knowledge will be forever loss due to personnel loss or turbulence. That the model does not capture this information is primarily a reflect of the fact that the doctrine writers for the operations of the AOC would not generally write about inter-personal professional development, personnel manning policies, and a myriad other sub-domains of knowledge that they take for granted. Text mining takes nothing for granted and is generally constrained to the *prima facie* evidence in the documents from which to draw inferences and conclusions.

The immediate impact analyses we performed only looked at the top ten nodes in specific measures when a key node was removed from the network. By only looking at the top ten nodes in specific measures, we limited our analysis to a small, exclusive set of nodes. We also, for the sake of reducing modeling complexity, did not extensively reflect information technology-mediate communications or the inter-connectedness of that technology. By avoiding the technology-dependent discussions, we reduced the complexity of the model, but we come perilously close to making a critical assumption: that IT systems may go off-line in single instances, but systemic failure is unlikely and therefore not contemplated.

The static network analysis used only singular removal of the top agents and roles in the AOC. What our analysis did not perform, but the model enables, is combinatoric analysis of the loss of one or more IT systems as well as key people/roles, or in an extreme case the loss of an organization—allowing determination of an interaction affects between these nodes. To become more confident in the resilience of an organization, there needs to be some appreciation by its members of the number and types of bad situations it can absorb while still being able to conduct its critical missions. Combinatoric exploration should support an analytic assessment of which systems, people, roles, processes, and knowledge have the greatest effects, singularly and in interactions. Armed with even simulated data, AOCs can make more informed decisions about how resilient they are and how to get to whatever threshold they have deemed acceptable.

Static Social Analysis can provide a snap-shot in-time analysis of a network. It can also given indicators about intermediate states between ‘everything normal’ and ‘everything is catastrophically broken.’ Using the model to conduct limited exploration of degraded states of operation would support commander’s desire to be confident in their continuity of operations (COOP) plans while avoiding impacts to on-going day-to-day requirements. Another aspect of the snap-shot in time the very different ways an AOC operates depending on where it and its supported forces are in the six-phase joint model of joint operations (i.e., Phase 0-Shape; Phase 1-Deter; Phase 2-Seize Initiative; Phase 3-Dominate; Phase 4-Stabilize; Phase 5-Enable Civil Authority). Impacts of various degraded states of operation will necessarily be a function where in those phases the AOC is working.

2.6 Conclusions and Implications of SNA and Modeling for Resilient AOCs

Modeling and running analysis on the AOC can reveal significant implications to the Air Force as well as the Combatant Command the AOC supports. More broadly, turning our analytic capabilities towards ourselves gives commanders another way of assessing organizational, personal, material, operational and training strengths and weakness. Importantly, the assessment can be non-invasive—that is the tools do not require days or weeks of exercises, war games, or otherwise detracting from daily functioning of the AOC.

The methods and tools used in this section can help identify ways to improve resilience in the face of contested cyber environments. In concert with other tools the USAF, as well as its Sister Services, uses, these methods can help identify areas of essential redundancy, less useful redundancy, and no- apparent-value redundancy. These techniques, if given a feedback loop into the Services' training and doctrine pipelines, can also help refine and improve the authoring and maintenance of documents that are supposed to be the touchstones of all Service members.

Combined with 'task-trackers' and experience built-up over careers, these techniques can support leaderships' decisions to distribute workload throughout the AOC as well as other organizations in supporting/supported relationships. While efficiency is not always the right goal of commander, it can frequently play a decisive role in internal and external resourcing decisions—having analytic tools to help assert integration and resilience can only decrease reliance on passion and intuition.

Every organization has centers of gravity. While the AOC and inter-AOC line-and-block diagrams give some indicators for center of gravity, the capabilities in ORA, AutoMap, and Construct can be used against enemy forces, they can just as interestingly be used in support of improving friend forces. Such self-views can help establish continuity of operations and disaster recovery (COOP/DR) plans –increasing the confidence of USAF commanders that their missions remain assured.

Finally, in the face of coming Service-wide budget cuts, having sets of tools that help forecast the impacts of task redistributions and realignments, as well as equipment changes in quantities and capabilities, can only improve the quality of the discussions leading to decisions. Through a sustained and broad-based effort to incorporate the myriad of tasks each unit must accomplish, in isolate as well as in coordination with others, we can build a more complete understanding of task work load at the organization as well as the individual levels. It is feasible that the intuition of 'too many faces, not enough places' reaction can be empirically shown in simulations, then incrementally tested in the AOCs before service-wide cuts cause permanent damage.

3 Simulating Integrated Resilient C2 in Contested Cyber Environments

Carnegie Mellon University (CMU) has several different ways of conducting simulations in support of assessing integrated resilient C2 in contested cyber environments. The first is integrated into ORA and is called Near Term Analysis (NTA). The section entitled Immediate Impact Reports Conclusions

Analysis of this model and this extreme case, a total denial of availability of four (4) key IT systems, in the context of the entire AOC, revealing a surprising but reassuring result: there are no catastrophic consequences predicted. This must be taken with a grain of salt however. The result is a snap shot in time, not a prediction over time. Equally important, the assessment assumes perfect assumption of communications by remaining IT systems and perfect adaptation by humans—neither of which is feasible without excellent continuity of operations plans and rehearsals of those plans.

When assessed exclusively in an IT-System ecosystem context, there are many SNA measures that are well past the 'suggestive' and 'meaningful' thresholds, some approaching a 50% drop in values from uncontested to contested environments. This is consistent with the perception of technologists that the AOC is extremely vulnerable to cyber attacks. Clearly, a contested cyber environment will affect elements of the AOC differently. The most important

lesson of this section is there is analytic support for Airmen who argue that 'the war will go in' even if the 'network is down.'

Near Term Analysis and Conclusions, in the last chapter, discussed NTA. The second method is through the use of Construct, an agent-based model (ABM) (Hirshman, Morgan, St. Charles, & M., 2010; C. Schreiber, Singh, & Carley, 2004). Construct is a validated information and belief diffusion simulation (C. Schreiber, et al., 2004) that allows researchers and modelers to extend social network analysis (SNA) into the longitudinal realm—allowing overtime analysis of how these networks, and the individuals that comprise them, may perform.

These kinds of dynamic network organizational models have helped decision makers, analysts, and researchers assess changes within and among organizational units. Illustrative applications at CMU include impacts of learning on organizational performance, merger assessment, leadership assessment, group performance, evolution of inter-organizational activity, and the assessment of terror groups. Other applications include identification of effective intervention strategies for counter-terror, counter-narcotic trafficking, and counter insurgencies (K. M. Carley; C. Schreiber, and Kathleen M. Carley, 2007).

3.1 Agent Based Models (ABM) and Construct

ABMs can simulate a group/organization (e.g. behavior, information flow, process flow, task execution). The "agents" in ABMs have agency – the ability to affect both themselves and others through their actions—thus earning their moniker. In dynamic network organizational modeling, the network is distinct from the spatial environment - there is no virtual grid upon which agents sit or that otherwise artificially constrain agents' behavior. Instead, agents occupy a multidimensional social topography where various socio-demographic, historical, technological and spatial considerations create and influence network relations. A combination of factors (social similarity, knowledge similarity, socio-demographic similarity, belief similarity, and physical adjacency) shape agents' interaction spheres and networks. This network topology may be static or dynamic as well as represent multiple networks (e.g. formal authority and informal friendships, alliance and adversarial networks). Depending on the researcher and questions of interest, the model can also represent organizational dynamics, such as personnel turbulence (e.g., moves, hiring, firing, and shift work) and training.

3.1.1 Construct, an Information and Belief Diffusion Model

In Construct, the agents, usually people (or at conceptually higher levels, groups or even countries), occupy a social network position that defines which other agents they can interact with. Construct operates at a middle level in terms of the cognitive realism of the agents, in that agents are boundedly rational and may not always correctly receive or interpret information from other actors, and at a high level in terms of the social realism of the agents through the implementation of well-known drivers of human interaction, homophily (the preference for interaction with similar individuals) and expertise-seeking. Key features of Construct are: sub-modules for various communication media including cyber media; multiple interaction logics based on fundamental well validated social principles of homophily-based interaction, expertise search based interaction, and co-work/collaboration interaction; instantiation via real data at a qualitative or quantitative level; and realistic inadvertent and intentional error models for the agents (K. Carley, Moon, Morgan, & Lanham, 2010).

Initialization of Construct can take the form of a mix of methods: using text-mined networks created through CMU's Automap capability; using meta-networks exported from CMU's ORA;

drawing networks from some other network analysis capability (e.g. UCINet, Pajeck); and creating artificial networks, such as any of the varieties of stylized networks, such as Erdös-Renyi, Scale-Free, Small-World, and Lattice networks.

3.1.2 Random Networks

As discussed in the chapter on Static Analysis using ORA (see also The Challenges of Doctrine with Text Mining), one of the difficulties associated with text-mined networks is whether the authors of the text corpus capture the organizational structure in the text. In this project, the Air Force doctrinal references were consistently good at describing the top-down links between the AOC divisions and their constituent teams. The various groups of authors were less consistent in enumerating the links between teams and their constituent cells. None of the source documents were consistent in explicitly stating how many people were in each cell, team, division, personal and special staff element. This lack of specificity led researchers to build a stylized model, inspired by the text-mined model, refined through referring back to source documents, and always operating with the realization that not a single AOC in the world is completely aligned with doctrine.

To mitigate the lack of explicit knowledge about the number of people per cell and per staff element, we picked as the default, six (6) Airmen per cell. We then created six rounds of Erdös-Rényi networks with a density of 50%. We then summed these six rounds to create a weighted network of these six agents. We designated the top two agents in betweenness centrality the cell leader and deputy leader. We then linked the team leader and deputy team leader, to whom the cell reports, to the three agents in the cell with the highest betweenness centrality. Though this method is not in strict accordnace to the doctrine, it allows the researchers to create a weighted asymmetric network at the lowest level of organizational structure the doctrine references.

3.2 Agent Based Model Data Description

The Construct model has a total of four AOCs compared to the static analysis' single AOC (see also Figure 2). As a simplifying measure, we modeled each AOC identically, though the authors acknowledge that the operations centers for each of the four commands are very different - unfortunately three of the four do not have doctrinal references describing their structure and operations.

To extend the single stylized network we discussed above to a total of four networks, we took several steps. We linked the TBMCS in each AOC to the others, replicating the linkages through SWIC. We also linked the GCCS in each AOC to the other three as well as JADOCS and C2PC. We used the underlying IT-resources to link intra-AOC nodes as well as inter-AOC nodes.

The stylized model also included a number of IT-resources that form the core of the underlying telecommunication infrastructure. We kept the IT-resource population to a minimal subset that allows us to begin exploring the impacts of the telecommunications networking links when combined with the social and usage network links. In Figure 18 below, it is important to note that we have begun recognizing that all IT-Resources and IT-Systems in the AOC are reliant on the commercial telecommunications company points of presence (TELCO_POP)—we omitted the various links to the multitude of military and commercial satellite links between AOCs. For the simulation, we treated IT-resources as mediating devices, but not as devices that could process data in the same was as IT-Systems such as TBMCS, GCCS, and others.

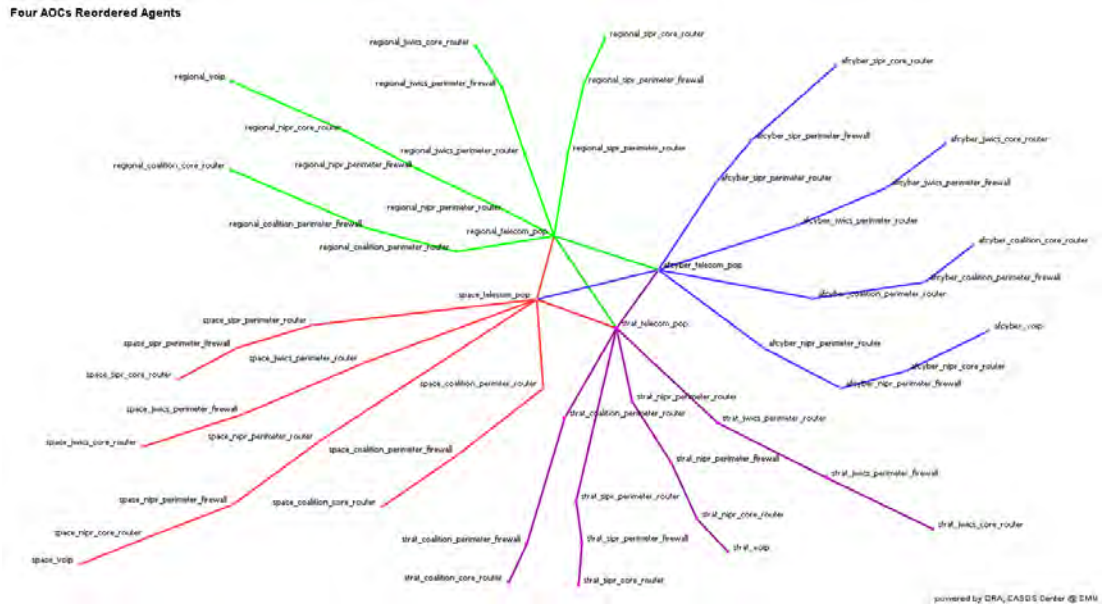

Figure 18 IT-Resource x IT-Resource Graph

We used the list of IT agents we harvested from the text mined data such that there were over 140 IT systems per AOC. As previously noted with respect to organizational links and team/cell composition, the text corpus was consistent for showing the links between IT systems. The D2M process does not rely exclusively on same-node by same-node matrices though, so the next two figures represent a picture of IT-System by IT-systems out of context of the entire AOC. Each figure uses the same color scheme as Figure 18.

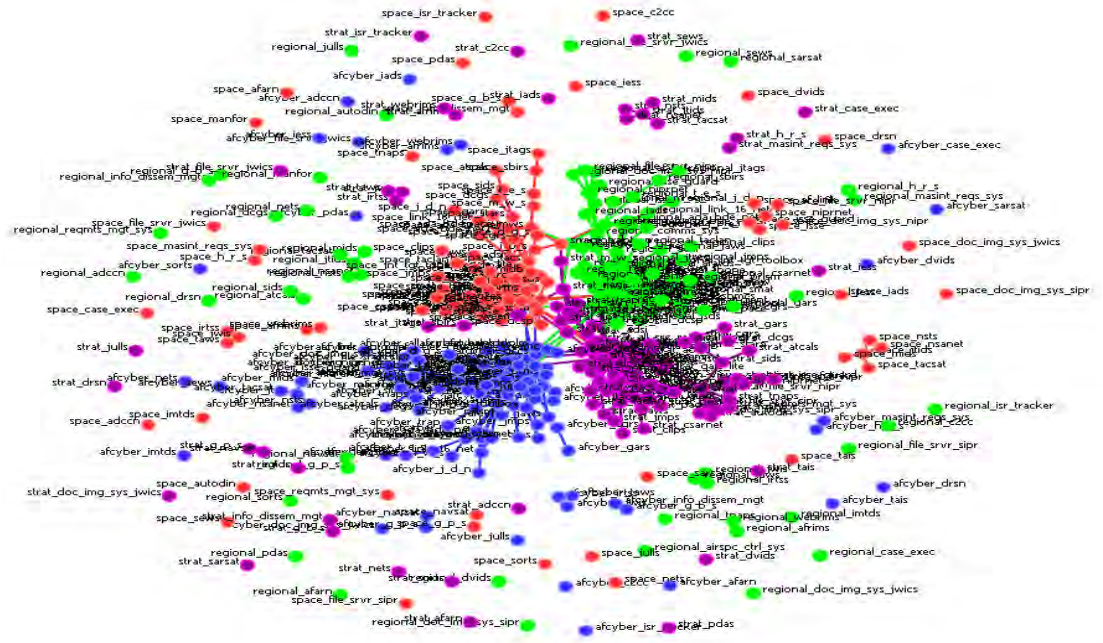

Figure 19 IT-System x IT-System network, including isolates

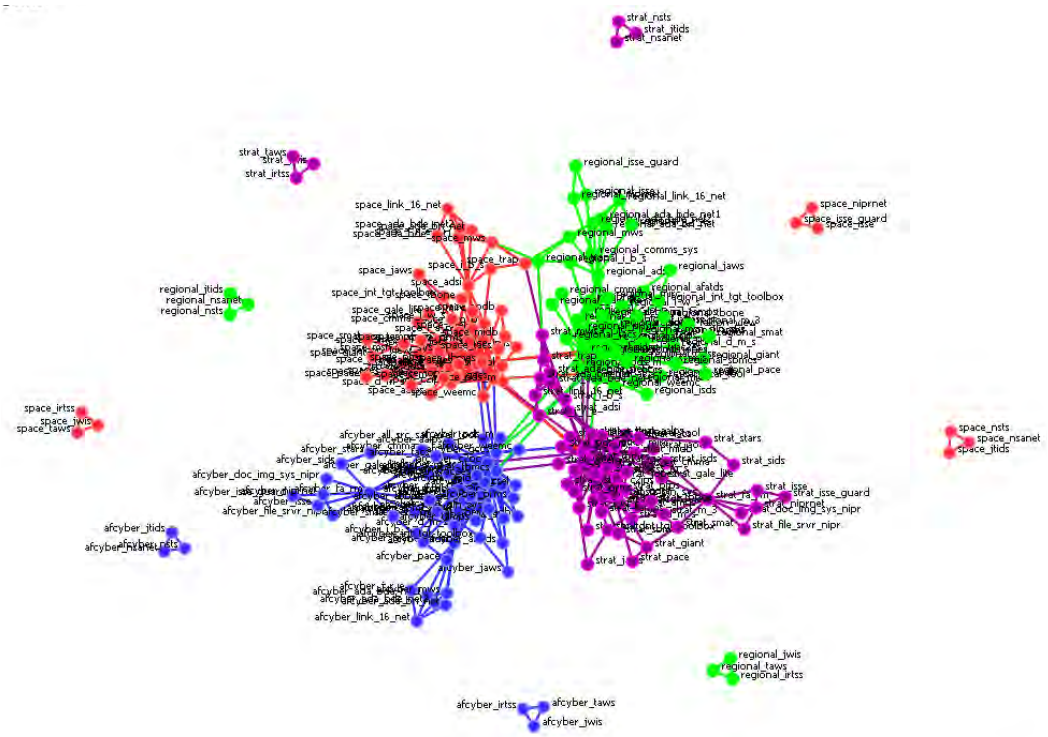

Figure 20 IT-System x IT-System network, without isolates

Finally, given there is no doctrinal reference from which we can draw social network data between AOCs, we created a small world network between the AOC Directors, the division heads, and the division deputy-heads.

3.2.1 Simulation Configuration and Execution

To simulate two types of contested cyber environments, we needed to pick which of several effects friendly forces could face. The five categories of Information Assurance provided a reasonable starting place for the conceptual binning of types of attacks. Those five categories are: Confidentiality, Integrity, Availability, Authentication, and Non-Repudiation. We implemented two forms of attacks that affected availability and integrity. We selected a cyber-event of a 30% degradation of DNS for IT Systems (without regard to which security domain those systems were part of). We also selected a cyber event of a loss of integrity in one or more of the top four systems: TBMCS, GCCS, C2PC, and JADOCS.

Because the doctrine, as analyzed, did not provide a sufficiently interesting set of knowledge bits with which to initialize the simulation, we specified knowledge for agents via a stylized but doctrinally sensitive method – resulting in several key classes of knowledge. The first was a set of knowledge bits that represented common USAF-culture knowledge. These thirty (30) bits were the basis for agents to assess and judge self-similarity to other agents. We then gave each AOC an additional thirty (30) bits representing the unique culture and interpretations of the world that each AOC has. We used random Gaussian distributions of knowledge assignment per agent with a mean of 50%.

We also created a doctrinally ill-defined group of agents that would be the primary mechanism from which the simulation would inject new knowledge into each organization. This group is the Joint Planning Group (JPG). For this project we designated two agents from the combat plans division, 2 from the ISR division and a layer for a total of five (5) JPG Members..

Referring back to Figure 1, note that the focus of the research was the integration of planning and operations between COCOMs (as implemented by George Mason University) and the integration of planning and operations between those COCOM's AOCs. As such, we developed a pool of knowledge bits that represented an integrated and coordinated operations order (OPORD) generated by the four COCOMs. This order is represented by 520 bits that accounts for each of the five paragraphs of an OPORD. Integrating this simulation with the GMU efforts, we allocated 30 bits to each of 14 actions in GMU's Pythia model (Pythia is a Time & Influence Network (TIN) a derivative of a Bayesian network). This resulted in a split of 90 bits directly affecting the Regional COCOM, 120 bits directly affecting JFCC-Space, 60 bits affecting USSTRATCOM, and 150 bits affecting AFCYBER. We had the simulator initialize itself with a 65% binary distribution of the JPG OPORD bits to the members of the JPG in each AOC (each agent has a 65% probability of having any particular bit of the 520 bits). To represent the electronic dissemination and distribution of an OPORD, we assigned 100% of the JPG OPORD bits to each of the four key IT systems.

JPGs usually execute a plan-brief cycle during the execution of their duties. To incorporate this cycle into the simulation, we have the JPG members in the simulation behave in two distinct patterns of behavior: planning behavior and briefing behavior. During planning behavior, the JPG members have a strong preference for interacting with each other and exchanging OPORD-related knowledge over general hemophilic knowledge. During briefing behavior, the JPG members have a strong preference for interacting with non-JPG members, without strong differentiation among the non-JPG members (this is contrary to a real-world JPG briefing where only select members of the AOCs attend the briefing).

During each interaction, agents can exchange different amounts of knowledge. Humans can initiate up to two interactions with other humans and IT systems. When interacting with fellow humans agents, humans can transfer 2-5 bits of knowledge. IT-Systems are effectively unlimited in the number of interactions it can participate in—IT systems are initiators and recipients of interactions so they are effectively push-pull systems. IT systems can transfer 5-15 bits of knowledge per interaction.

3.2.2 Simulation Virtual Experiments

To configure the simulation for the degradation of DNS, we had the simulator create a random binary distribution across all the IT-systems' access network with a mean of 70% (see also Appendix 1 and Appendix 2). Every edge that existed in the uncompromised environment had a 70% chance of being active each turn, with the activity of the edge being defined turn by turn.

To configure the simulation for the integrity attack, we implemented a special agent that was not part of any doctrinal document. We configured this agent to have access to 'bad knowledge' and when the integrity attack was enabled, we allowed the special agent to interact with one or more of the four key IT-Systems. We set the amount of 'bad knowledge' to be half of the bits representing the OPORD for a total of 210 bits. Possession of these bits provide a means of assessing the diffusion of 'bad knowledge' with the mathematical effect of negating the quantity of JPG knowledge agents in the AOC possess.

Finally, we established a total of 27 experimental conditions, for which we ran 20 iterations of each condition to establish a range of output values and better assess changes' significance. Our base line condition was an uncontested environment. Our first cyber attack affected the DNS reliability, with the concurrent and effect-of-interest being some random 30% of IT-Systems

could become unavailable for use. DNS reliability could affect either *only* the Regional AOC or all four AOCs. Omitting the case of combinations of 2 and 3 AOCs allowed for a simplification of the overall experiment. The second cyber attacked is an integrity attack where one, a combination of 2, or all four IT-Systems would be exposed to the 'bad information' attack. Integrity attacks could affect either *only* the Regional AOC or all four AOCs. These two combinations of attacks, limited to the following IT-Systems combinations (TBMC & GCCS [TG], GCCS & C2PC [GC], C2PC & JADOCS [CJ], and all four [TGCJ]).

3.2.3 Measures of Interest for Assessing Resilience

In the previous chapter, we assessed resilience through an evaluation of percentage changes in numerous measures of interest. Insensitivity to various conditions (e.g., deletion of an IT-System or combination of systems, isolation of a human agent(s)) is a mark of resilience when we refer back to the definition of mission assurance the USAF is promulgating.

Specific measures that are immediately useful include task and resource congruence; fragmentation through loss of agent(s); communication speed degradation (e.g., as measured through SNA techniques, not telecommunications analytics or bandwidth); diffusion degradation; performance degradation; number of people with minimum ability to operate; and the ability to complete planning. It is these last two that provide the basis for evaluation of the simulated model.

3.2.4 Comparative Analysis of Virtual Experiments

The simulation did not reach, in the 120 time periods we simulated, 100% diffusion, nor was that a primary goal for the modeling effort. Instead of focusing on the degree of perfect diffusion, the authors assess the difference between the baseline performance of the simulation and the performance in each of the virtual experiments. To make the comparisons simpler, we normalize the outputs of each experiment by dividing the measure of interest by the value of that measure in the baseline.

The figures below begins to show a consistent result: integrated AOCs are more resilient than an single AOC; the non-linear effects of integrity attacks combined with availability attacks across all four AOCS were more effective than other attacks. In Figure 21 and Figure 22, there is a short-hand we used to identify each experimental condition. We labeled the DNS attacks as "Reliability." A "M" prefix in front of *reliability* indicates a Regional-AOC only attack while a "T" prefix in front of *reliability* indicates a total attack across all four AOCs. The letters in parenthesis at the end of each label represent the IT-System affected by the attack. The number of systems gives an indication of whether the integrity attack is Regional AOC only or global.

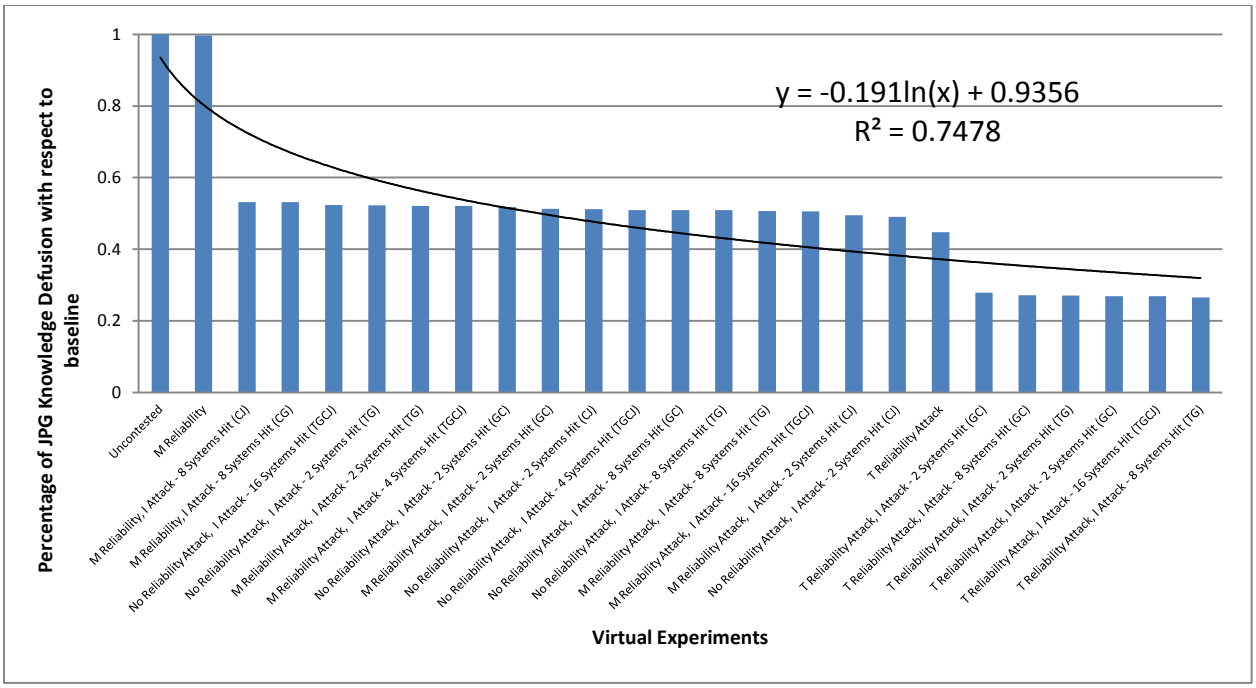

Figure 21 Average JPG Knowledge Score relative to baseline, 1/3 of experiment completed (40 time periods)

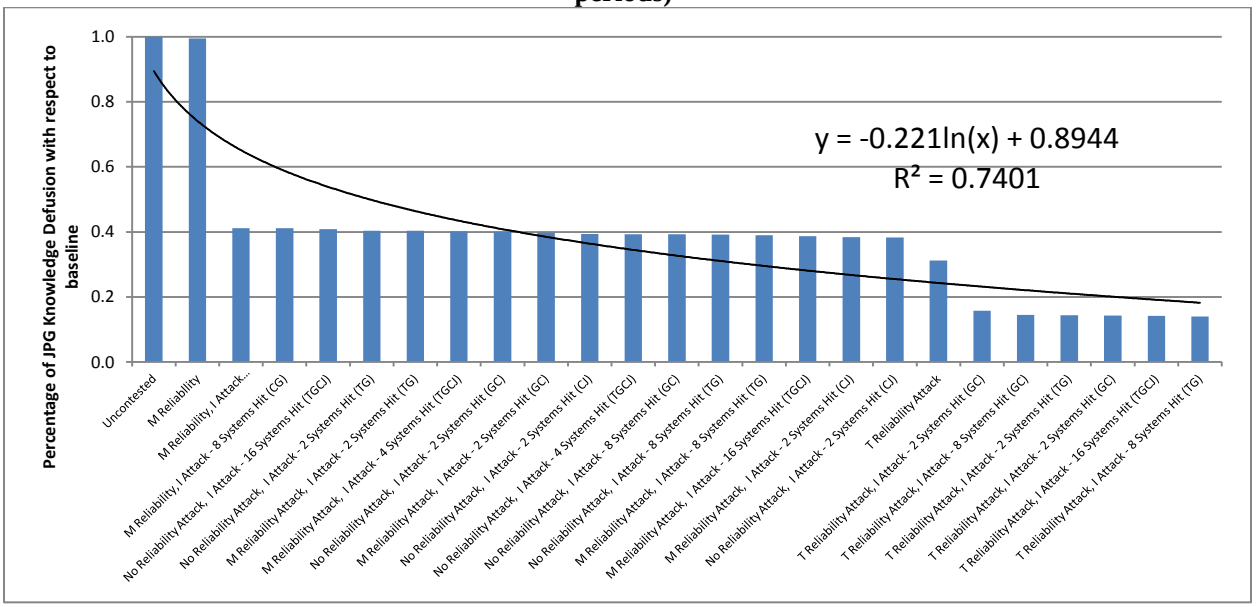

Figure 22 Average JPG Knowledge Score relative to baseline, at end of the experiment (120 time periods)

Another way of representing these results is shown in Figure 22, where the non-linear relationship between the number of attacks and the change in percentage is clearer, though the nature of specific attacks is obscured.

Figure 24 shows a key and useful outcome for this project. Degradation achieved within a single AOC was shown to be over 30% from baseline, but when expanding the scope of analysis

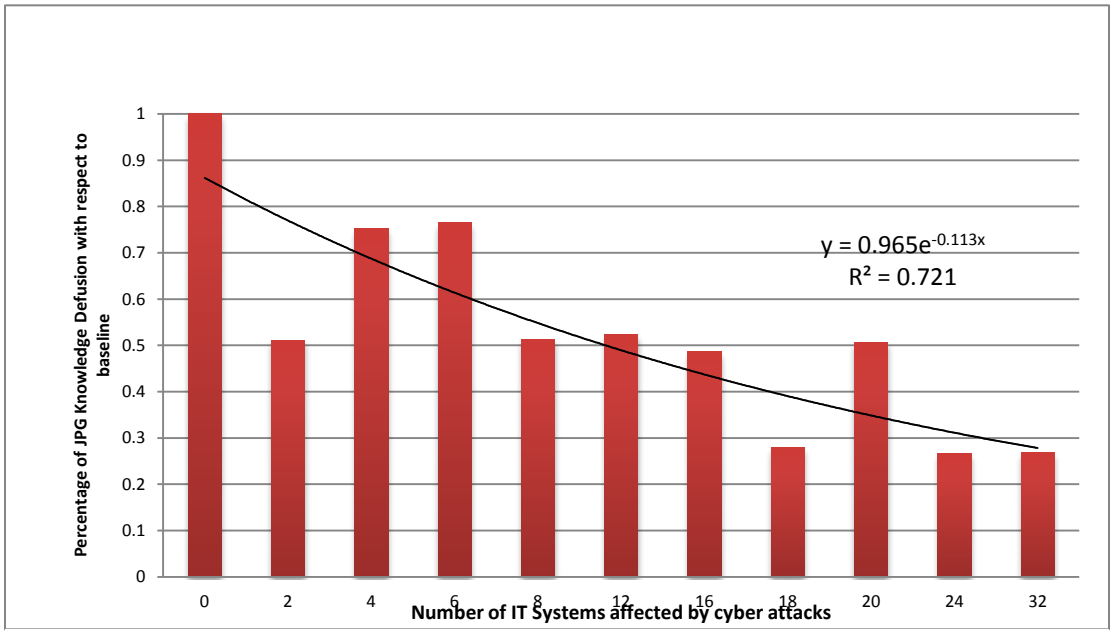

Figure 23 Number of IT systems affected by cyber attacks

to the 4 x AOC system, degradation was not a linear effect, instead it shows that multiple AOCs sharing the same integrated OPORD can mitigate against both single-AOC attacks as well as multi-AOC attacks.

Figure 24 is depicting the familiar pattern seen in the static analysis from the previous chapter. Deleting or impacting multiple IT-systems has a non-linear effect on the resilience of the AOC system. This figure is depicting the change in two (2) network measures, number of isolated agents and fragmentation. The important thing to note from Figure 24 is to reduce the impact of cyber-events, an AOC should work at increasing the links between its people and the organization's knowledge. This recurring non-linear effect is consistent across several different measures with Figure 26 showing the same kind of behavior with five (5) additional network measures: performance as accuracy; diffusion; clustering coefficient; density; and average communications speed.

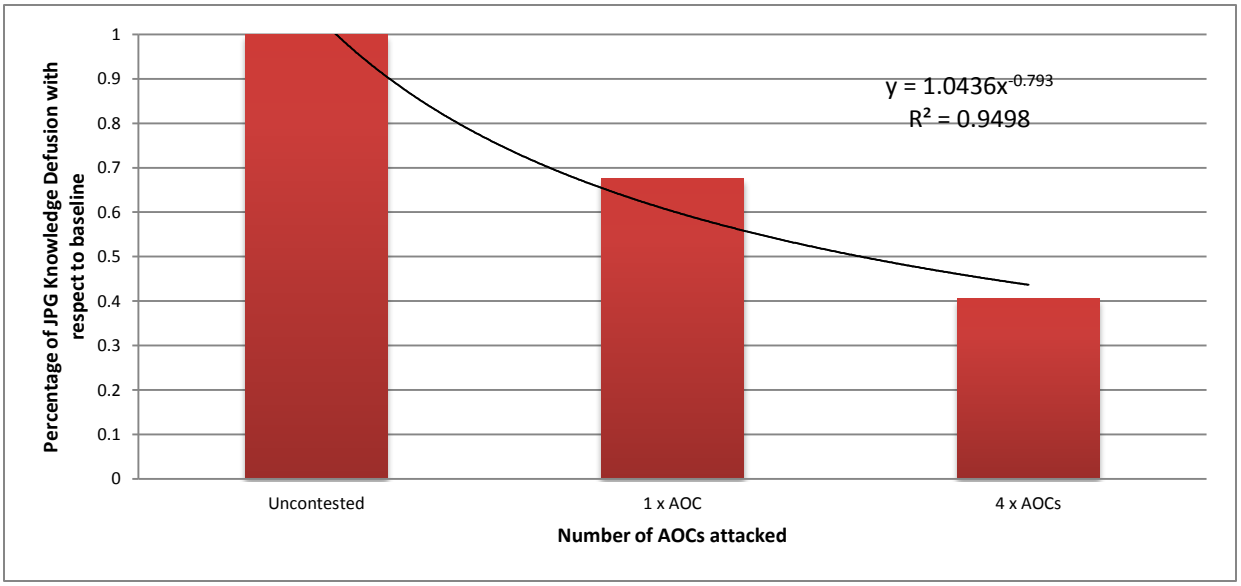

Figure 24 Integrated AOCs increases resilience

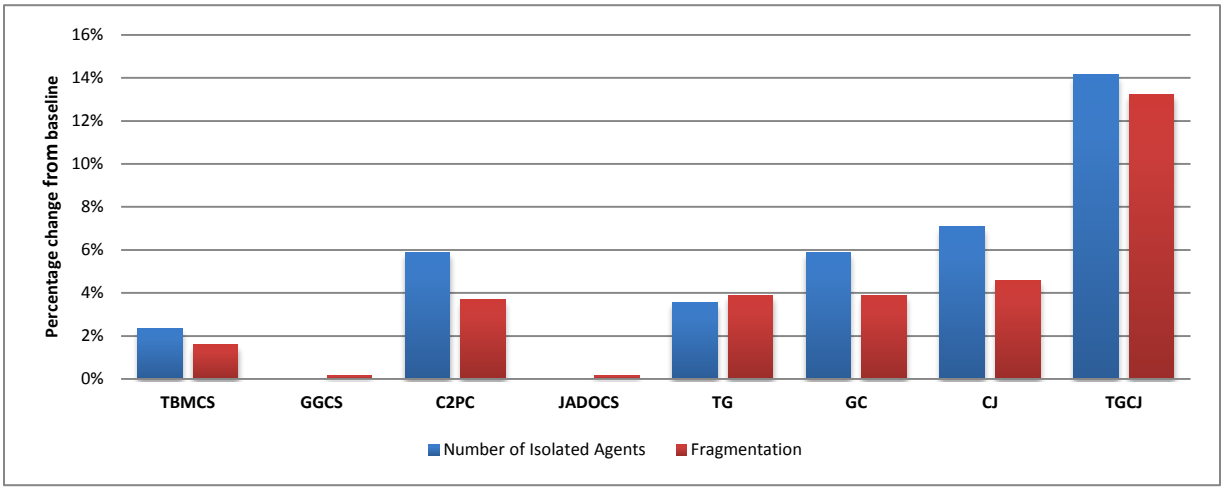

Figure 25 Two (2) Network Measures Change from Baseline

The simulations were each run for 20 iterations per virtual experiment. Each experiment is independent of all other experiments and is capable of generating different results. There was a difference between the maximum diffusion we saw in these runs, and the average. Below, we see that the average diffusion in the uncontested environment, compared to the maximum, was not 100%--indeed, for a single AOC, it averaged close to 60% and for the 4 x AOC model it average closer to 70%. In Figure 27, the bar chart shows a polynomial relationship between the uncontested environment, a reliability attack, an integrity attack, and a combination of both. A data point to consider is that as additional attacks occur, the standard deviation increases as shown in Figure 27.

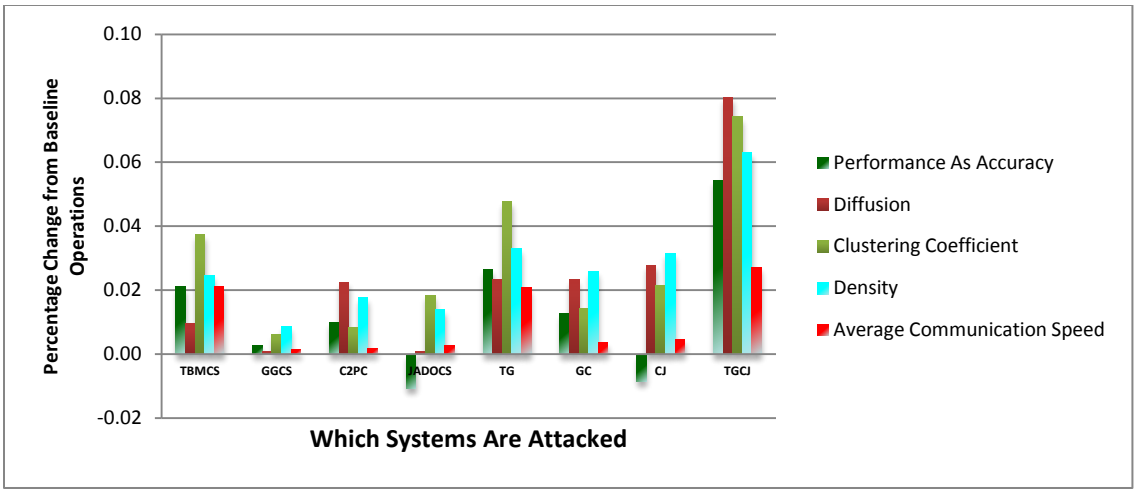

Figure 26 Five (5) Network Measures Changes from Baseline

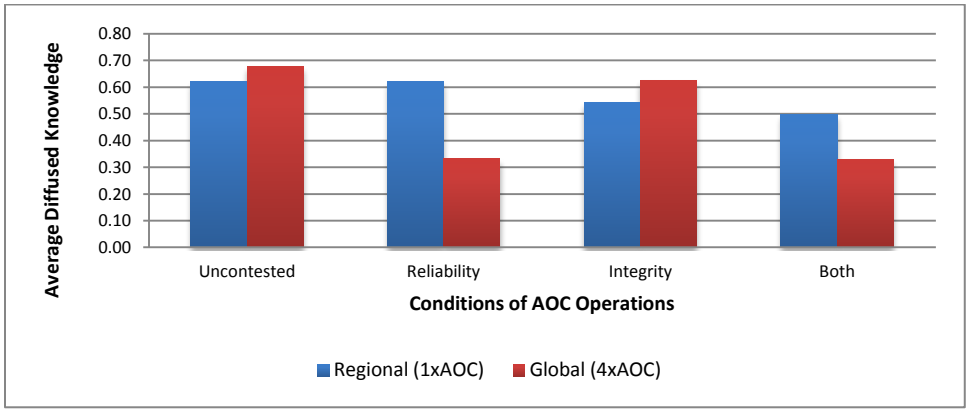

Figure 27 Average Diffusion of Knowledge as a Percentage of baseline, across four modes of operations

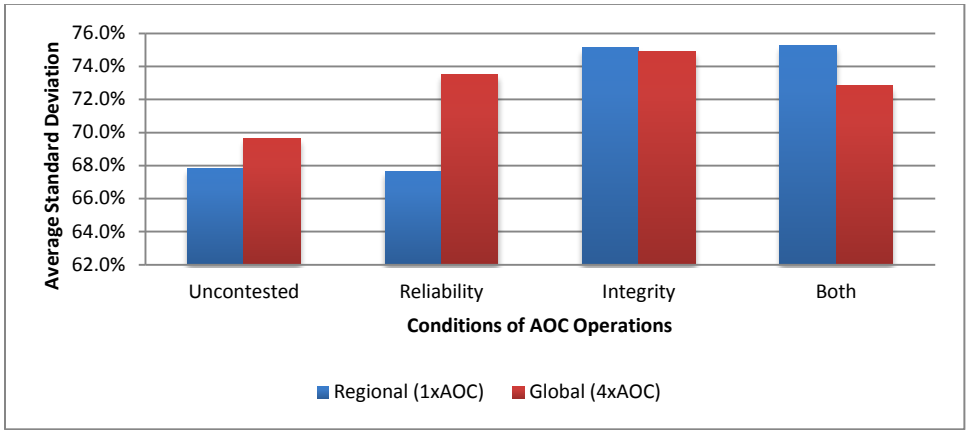

Figure 28 Average Standard Deviation as a Percentage of baseline, across four modes of operations

3.3 Discussion and Contributions from Simulations of Integrated AOCs

This effort, as part of a multiple research center project, has demonstrated the value of integration of multiple commands as a mitigation against cyber attacks against a single command as well as against multiple commands. While abstracting away the technical complications of

telecommunications infrastructure, this model provides analytical support to the USAF decision to develop resilient organization through the strength of their personnel. Personnel come, automatically and with little direct costs to the Air Force, with social networks. When commands and organizations use these inherent social networks as part of their organization design, this model makes the strong suggestion that they become much more resistant to cyber events.

The effort also contributed to a better understanding of domain specific text mining and how to accommodate some of the vagaries of DoD doctrinal documents. We explored several ways of mitigating the presence of diagrams, tables, and figures and were able to quantify the results and advantages of doing so.

We have shown ways of bridging the gap in doctrinal documents between the discussions of organizational structure and incorporating social networks into the model. Through the use of random stylized networks, we were able to develop interaction networks for individual agents within the cells of the AOC.

3.4 Future Work

The authors, with permission, developed a simplified model that made each AOC identical. From this initial effort, a deliberate effort should be made to modify the structure of each AOC to more closely align with the way each AOC sees itself. The process of aligning the model of each AOC with the as-built versions of the commands' AOCs/Operations Centers would allow several things: a comparison between as-designed and as-built for each AOC; a comparison between this universal design and a multi-design model to substantiate the use of general models; and increasing the face-value plausibility of the static and stylized models.

Figure 2 showed, related but not tightly coupled research efforts between GMU & CMU. Both research centers should expand the scope of future efforts to incorporate the bi-direction communications between COCOM HQs and their operations centers. The expansion of the scope of the model will allow a more detailed examination of cyber events in the context of an entire set of commands, without the simplifying assumption that each organization was an island unto themselves.

Neither the CMU nor GMU models incorporate shift work. Shift work brings its own challenges to any organization, not least of which are the shift-change briefs at the end/beginning of each shift. The model as built, where all agents can interact with each other regardless of the shift they are on, does not capture the complexity of maintaining shared knowledge across shift barriers. Nor does it directly incorporate the communications overhead associated with doubling a shift's population, nor the long term performance drop of shift workers taken out of their normal operating cycles. Shift work virtual experiments should incorporate at least two shift schedules: Day/Mid/Swing and Day/Night. Developing this additional complexity in the model will increase the face validity of the model as shift workers are generally not conducting face-to-face interactions except for short duration, high volume interactions (shift-change briefs).

We operationalized the diffusion of knowledge in these AOCs by simulating the broad process of receipt of a common OPORD and then conducting the Joint Planning Process (e.g., plan-brief cycle). However, depending on the current and anticipated operational phase of the organization, commanders may be willing to work in trade spaces they are usually not comfortable with. For example, if AOCs are in the middle of Phase 3 operations, leaders will likely be loath to accepting high risk mitigation strategies. The same strategies may be low or medium risks if the command is in the middle of Phase 5, support to civil authorities.

Construct has a task-based interaction mechanism that does not have the capacity to mimic time-limited and task-prioritized tasks. Future simulations that incorporate such a capacity would automatically be able to help with the observation from the paragraph above—different phases of a campaign can drive different results and solutions to the observed problem.

Construct has an asynchronous communications mechanism in the form of email. We did not use this technique in this simulation. Future efforts at developing the simulation should consider not only email, but other methods of asynchronous communication. In addition to asynchronous technology such as email, or the DoD AMHS, modelers should include the more full bodied IT communications infrastructure. All tech-related interactions are mediated with one or more computer terminals. To gain a more complete model, future researchers must include the several thousand items of glassware.

Future work should also attempt to identify if there is a tipping point where if a single additional node or system becomes unavailable or less functional, some form of cascading failure is triggered. Cascading failures in electric power systems are well studied, but not nearly so when it comes to organizational performance over time.

3.5 Conclusions

The most essential conclusion of this effort is that the AOC, as defined by its doctrinal references is surprisingly resistant to cyber-disruption and attack. When analysis incorporates more than single organizations or single types of entities, completely different results are not only feasible, but extremely likely: recall that from an IT-centric viewpoint, deletion of 4 IT systems created dramatic impacts but those same deletions, when viewed from the entire AOC viewpoint the deletion caused fewer changes to network measures.

We provided an analytical basis to assert that integrated AOCs are more resilient than stand-alone organizations. Though there is always a danger that a too tightly coupled integration will lead to easily triggered cascading failure, we have no indication yet of where that point may be—we did not reach it in this simulation. This finding, in many ways, runs counter to the DoD's tendency to slice responsibilities up between different organizations. That tendency is an outgrowth of the desire to maintain clear lines of authority and responsibility which are well established military axioms.

We also provided the beginnings of an analytic approach that may reduce the number of *Chicken Little* declarations in the cyber and IT domains. It is almost a professional requirement for all serious practitioners of IT security to assert the status quo is a failure or ready to have the sky fall down on its head. There are many people in the status quo who have equally passionate opinions on the threat to our future being over blown and/or exaggerated. Though the actual answer to the question of "How much security do we need?" will likely remain an ever moving target, an analytical answer is more useful than an emotive answer.

Increasing the probability that Airmen and other members of the DoD know each other, or are one separated by one or two degrees can increase resiliency. Familiarity with others in distant locations can increase the level of trust and confidence that messages and communications have been passed and been commonly understood. With that trust and confidence, temporary, or longer-term communications outages can be weathered with less angst.

At a 2011 USAF war game a participant stated, with great succinctness and clarity of thought: "So the networks and systems are fried, it's not like the war's going to stop." He went

on to point out that 8th Air Force during WWII put hundreds of plans into the air virtually every day with nary a computer in sight - we can do it again, though it will be painful getting there.

4 References

24th Air Force Public Affairs. (2011, circa August 2009). 24th Air Force - Units Retrieved 2 May, 2011, from http://www.24af.af.mil/units/index.asp

Abreu, Elinor. (2001, 9 May 2001). Cyberattack Reveals Cracks in the U.S. Defense. *PC World*.

Carley, Kathleen M. Adaptive Organizations and Emergent Forms.

Carley, Kathleen M., Columbus, Dave, Bigrigg, Michael, & Kunkel, Frank. (2011). AutoMap User's Guide 2011 *[Technical report] / Carnegie Mellon University School of Computer Science Institute for Software Research International CMU-ISRI-11-108*. Pittsburgh, Pa.: Carnegie Mellon University, School of Computer Science, Institute for Software Research International, Pttsburgh PA 15213.

Carley, Kathleen M., Columbus, Dave, DeReno, Matthew , Reminga, Jeff , Storrick, Jon, & Columbus, Dave. (2011). ORA User's Guide 2011: Carnegie Mellon University, School of Computer Science, Institute for Software Research.

Carley, Kathleen, Moon, Il-Chul, Morgan, Geoffrey, & Lanham, Michael (2010). Adversary Modeling –Applications of Dynamic Network Analysis. In Kathleen M. Carley & Alexander Levis (Eds.), *Computational Modeling of Cultural Dimensions in Adversary Organizations* (pp. 172-203). Fairfax, VA: The Volgenau School of Engineering Dept. of Electrical and Computer Engineering System Architectures Laboratory, George Mason University, Technical Report.

Committee on National Security Systems (CNSS). (2010). (CNSSI) National Information Assurance (IA) Glossary (U) (Vol. CNSSI-4009). Ft Meade, MD: CNSS Secretariat, NSA.

Gates, Robert. (2009). *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations*. Washington, D.C.: OSD Retrieved from http://online.wsj.com/public/resources/documents/OSD05914.pdf.

Goldwater-Nichols Department of Defense Reorganization Act of 1986, Cornell Law School Legal Information Institute, Pub. L. No. 99-433 § Subtitle A, Part I, Chapter 5 Sect. 151 (2010 1 Oct 1986).

Hirshman, Brian R., Morgan, Geoffrey P., St. Charles, Jesse R., & M., Carley Kathleen. (2010). Construct Demo Input Deck (Institute of Software Research School of Computer Science, Trans.) (pp. 149). Pittsburgh, PA: Carnegie Mellon University.

Joint Staff J3. (2006). *Information Operations*. Washington, D.C.: Joint Staff Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf.

Joint Staff J7. (2010). *Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C.: Joint Staff Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

Levis, Alexander H., Carley, Kathleen M. , & Karsai, Gabor. (2011). Resilient Architectures for Integrated Command and Control in a

Contested Cyber Environment (System Architectures Laboratory, Trans.) (pp. 169).

Lynn, William J. III. (2010). Defending a New Domain. [Essay]. *Foreign Affairs*, *89*(5), 97-108.

Paone, Chuck. (2000). Combined Air Ops Center Features AFMC, ACC Teams. *European Security and Defense*, 1. Retrieved from European Security and Defense website: http://www.european-security.com/index.php?id=1346

Parrish, Karen. (2011). General Cites Cyber Domain Challenges. Retrieved from http://www.defense.gov/News/NewsArticle.aspx?ID=65722

Pike, John. (2011, 05-07-2011 06:35:18 Zulu). Solar Sunrise Retrieved 17 October, 2011, from http://www.globalsecurity.org/military/ops/solar-sunrise.htm

Schreiber, C., and Kathleen M. Carley. (2007). *Agent Interactions in Construct: An Empirical Validation using Calibrated Grounding*. Paper presented at the 2007 BRIMS, Norfolk, VA.

Schreiber, Craig, Singh, Siddhartha, & Carley, Kathleen M. (2004). Construct - A Multi-agent Network Model for the Co-evolution of Agents and Socio-cultural Enviroments *[Technical report] / Carnegie Mellon University School of Computer Science Institute for Software Research International CMU-ISRI-04-109* Retrieved from http://www.casos.cs.cmu.edu/publications/papers/schreiber_2004_constructmultiagent.pdf

Shackelford, Scott J. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. [Accepted Paper Series]. *Berkley Journal of International Law (BJIL), 25*(3), 60.

USAF. (2005). *Air Force Instruction (AFI) 13-1AOC, Operational Procedures - Air and Space Operations Center (AOC).* Langley AFB: HQ USAF/XOOY Retrieved from http://www.af.mil/shared/media/epubs/AFI13-1AOCV3.pdf.

Webber, Richard E. (2010). *Mission Assurance, Changing the Mindset*. Paper presented at the Global Warfare Symposium, Beverly Hills, CA 90210. http://www.afa.org/events/natlsymp/2010/scripts/101118-Webber.pdf

Appendix 1 – Encoding Scheme for Ontological Classification

Key word/words in original text segment	metaOntology category
request	Action
Chief, commander, database, director, system, processor, tool	agent
Specific named people relevant to project, Specific named position within orgs filled by exactly one person (e.g., Commander, Director, Secretary)	agent
Critical	belief
Conference	event
Agreement, Architecture, consequence, contract, course, day, Estimate[2], guide, handbook, instruction*, law, memo, memorandum, message, mission[3], Module[4], plan, policy, program, programme, report, treaty	knowledge
Shared information, if when given to another, the originator still has the information	knowledge
Area, Facility, installation, base, operations area, station	Location ("station" when in context of physical location, else likely a task "to station")
Program	Often task (e.g., WMD Counter-proliferation), sometimes organization (e.g., in context of a Program Office) , sometimes knowledge (e.g., a program given out at beginning of an event)
Agency, branch, brigade, center, committee, company, council, detachment, division, fleet, MEU, MEB, Mission, *office*, office for, office of, organization, platoon, program office, *service*, ship, squadron, team, united, wing,	Organization (specific ships, when discussed as a resource [e.g., USS JFK was decommissioned/overhauled) get coded as "resource" instead of org)
A collection of people or organizations (by composition or aggregation)	organization (e.g., fighter wing, division, brigade, agency)
Element	organization or knowledge
Causeway, equipment, fuel, medal, missile, package	Resource

[2] When in context of an estimate of the situation, a deliverable product, not a task to conduct an estimate
[3] usually knowledge, but sometimes a 'task'
[4] in context of a course module. When used in sense of 'component of a whole,' it's a resource

Computer systems	resource – if single user or =’knowledge’ is lost when an agent is no longer in possession of the computer system agent – if it passes knowledge/information between other agents/organizations. Using computers imposes a cognitive load on people as well. Finally, intention is to model within construct the following: p(forgetting)>0 & << 1; p(! interact) >0 & << 1; p(tx err)>0 & << 1.
An instance of a physical asset, if when given to another, the originator no longer has it	resource (e.g., an actual ship, an actual aircraft)
Guided	resource (usually in context of guided weapon)
Non-specific position within orgs (e.g., officer, assistant secretary [without a qualifier])	role
Foe[5], Management[6], process , reception, responsibilities, , support, task, Estimate[7]	task
Acronyms <= 3 chars	insert underscore between letters

[5] In context of identify friend or foe, else agent or role
[6] In context of a task, when part of a title it usually becomes part of an n-gram and organization
[7] when a task to conduct an estimate of a situation, otherwise ‘knowledge’

Appendix 2 – Construct Configuration File (construct.xml)

Note to the reader: As a space conservation measure, we modified the indentation of the printouts in Appendix 1, 2, 3, and 4. Future users, should they desire to use the code, can paste it into their favorite source code editor and use the formatting function of the editor to return to a more normal indentation convention for source code.

```
   <construct>
      <!-- This is for CMU/GMU Resilient/Integrated C2 Project Collaboration
      Demonstration scheduled for Week of 24 Oct-->
      <construct_vars>

      <!-- ############# Start vars from parameters file ############## -->
      <var name="param_val_col" value="1" />
      <var name="human_agent_end"
        value="readFromCSVFile[params.csv,0,construct::intvar::param_val_col]" />
      <var name="ITSystems_count"
        value="readFromCSVFile[params.csv,1,construct::intvar::param_val_col]" />
      <var name="ITResources_count"
        value="readFromCSVFile[params.csv,2,construct::intvar::param_val_col]" />
      <var name="DNS_FMC_All"
        value="readFromCSVFile[params.csv,3,construct::intvar::param_val_col]" />
      <var name="DNS_FMC_Regional"
        value="readFromCSVFile[params.csv,4,construct::intvar::param_val_col]" />
      <var name="Integrity_Attacks_Per_Turn"
        value="readFromCSVFile[params.csv,5,construct::intvar::param_val_col]" />
      <var name="TBMCS_Attacked_All"
        value="readFromCSVFile[params.csv,6,construct::intvar::param_val_col]" />
      <var name="TBMCS_Attacked_Regional"
        value="readFromCSVFile[params.csv,7,construct::intvar::param_val_col]" />
      <var name="GCCS_Attacked_All"
        value="readFromCSVFile[params.csv,8,construct::intvar::param_val_col]" />
      <var name="GCCS_Attacked_Regional"
        value="readFromCSVFile[params.csv,9,construct::intvar::param_val_col]" />
      <var name="C2PC_Attacked_All"
        value="readFromCSVFile[params.csv,10,construct::intvar::param_val_col]" />
      <var name="C2PC_Attacked_Regional"
        value="readFromCSVFile[params.csv,11,construct::intvar::param_val_col]" />
      <var name="JADOCS_Attacked_All"
        value="readFromCSVFile[params.csv,12,construct::intvar::param_val_col]" />
      <var name="JADOCS_Attacked_Regional"
        value="readFromCSVFile[params.csv,13,construct::intvar::param_val_col]" />
       <var name="gsphere_fname"
        value="readFromCSVFile[params.csv,14,construct::intvar::param_val_col]" />
      <var name="Time_UpScale_Factor" value="1" />
      <!-- as of Oct '11, Construct having trouble reading in float vars. So
        convert the read-in Integer to a float and make it a decimal -->
      <var name="DNS_FMC_All_Float" value="construct::floatvar::DNS_FMC_All / 10.0 "
/>
      <var name="DNS_FMC_Regional_Float"
value="construct::floatvar::DNS_FMC_Regional / 10.0 " />
      <var name="time_count" value="120" />
      <!-- Keep divisible by 3 & 4 as output is a function of quartiles and
        JPG meetings are a function of thirds (when they happen) and have
        a duration function of 20ths -->

      <!-- ############# Start Agent definitions ############## -->

      <var name="agentgroup_count" value="0" />

      <!-- Human Agents IDs by group -->
      <!--  ASSUMPTION:  AGENTS ARE IN CONSECUTIVE GROUPS -->
      <!--  AOCs -->
      <var name="AFCyber_begin" value="0" />
      <var name="AFCyber_end" value="396" />
      <var name="Regional_begin" value="construct::intvar::AFCyber_end + 1" />
      <var name="Regional_end" value="793" />
      <var name="Space_begin" value="construct::intvar::Regional_end + 1" />
      <var name="Space_end" value="1190" />
      <var name="Strat_begin" value="construct::intvar::Space_end + 1" />
```

```
        <var name="Strat_end" value="1586" />
        <var name="JPG_begin" value="construct::intvar::Strat_end + 1" />
        <var name="JPG_end" value="1606" />

        <!-- ASSUMPTION: JPGs are end of all AOC Agent lists. JPGs are
          in the same AOC-order as the AOCs themselves. -->
        <var name="JPG_Size" value="5" />
        <var name="AFCyber_JPG_begin" value="construct::intvar::JPG_begin" />
        <var name="AFCyber_JPG_end" value="construct::intvar::AFCyber_JPG_begin
          + construct::intvar::JPG_Size - 1"/>
        <var name="Regional_JPG_begin" value="construct::intvar::AFCyber_JPG_end
          + 1" />
        <var name="Regional_JPG_end" value="construct::intvar::Regional_JPG_begin
          + construct::intvar::JPG_Size - 1"/>
        <var name="Space_JPG_begin" value="construct::intvar::Regional_JPG_end + 1" />
        <var name="Space_JPG_end" value="construct::intvar::Space_JPG_begin +
          construct::intvar::JPG_Size-1"/>
        <var name="Strat_JPG_begin" value="construct::intvar::Space_JPG_end + 1" />
        <var name="Strat_JPG_end" value="construct::intvar::Strat_JPG_begin +
          construct::intvar::JPG_Size-1" />

        <!-- ASSUMPTION: ITResources are, as of Sep '11, essentially
          pass-through agents. They have perfect transmission, no errors,
          always connect to others as "pull" IT systems -->
        <var name="ITResources_begin" value="construct::intvar::JPG_end + 1" />
        <var name="ITResources_end" value="construct::intvar::ITResources_begin
          + construct::intvar::ITResources_count - 1" />

        <!-- ASSUMPTION: ITSystems are, as of Sep '11, store and forward agents.
          They have perfect transmission, no errors, always connect to others
          as "push/pull" IT systems -->

        <var name="ITSystems_begin" value="construct::intvar::ITResources_end + 1" />
        <var name="ITSystems_end" value="construct::intvar::ITSystems_begin +
          construct::intvar::ITSystems_count-1" />


        <!-- ITResource Agent IDs -->
        <!-- ITResources used to start right after human agents end, now we
          treat them as human_agents -->
        <var name="ITResource_agent_begin"
value="construct::intvar::ITResources_begin" />
        <var name="ITResource_agent_end" value="construct::intvar::ITResources_end" />


        <!-- ITSystem Agent IDs -->
        <!-- IT Systems start right after IT Resources end -->
        <var name="ITSystem_agent_begin" value="construct::intvar::ITSystems_begin" />
        <var name="ITSystem_agent_end" value="construct::intvar::ITSystems_end" />

        <!-- ASSUMPTION, the top 4 families of IT Systems (in Key Entity
          Reports) are the last ones in the list.  Each of 4 AOCs has these
          systems, so this is the first 16 IT systems -->

        <!-- Special IT Systems in this simulation have starting perfect task
          knowledge, hence the reason we differentiate Special IT systems from
          Normal IT Systems -->
        <var name="SpecialITSys_count" value="16" />
        <var name="SpecialITSys_begin"
          value="construct::intvar::ITSystem_agent_end -
          construct::intvar::SpecialITSys_count" />
        <var name="SpecialITSys_end" value="construct::intvar::ITSystem_agent_end" />

        <var name="TBMCS_All_begin" value="2122"/>
        <var name="TBMCS_All_end" value="2125"/>
        <var name="GCCS_All_begin" value="2126"/>
        <var name="GCCS_All_end" value="2129"/>
        <var name="C2PC_All_begin" value="2130"/>
        <var name="C2PC_All_end" value="2133"/>
        <var name="JADOCS_All_begin" value="2134"/>
        <var name="JADOCS_All_end" value="2137"/>


        <!-- Normal IT Systems in this sim have starting imperfect task knowledge,
          but are capable of learning the additional knowledge bits -->
```

```
      <var name="NormalITSys_begin" value="construct::intvar::ITSystem_agent_begin"
/>
      <var name="NormalITSys_end" value="construct::intvar::ITSystem_agent_end -
construct::intvar::SpecialITSys_end" />


      <!-- Special Agent IDs -->
      <!-- Being used for this simulation as the bad actor -->
      <var name="special_agent_count" value="1" />
      <var name="special_agent_begin" value="construct::intvar::ITSystems_end + 1"
/>
      <var name="special_agent_end"
        value="construct::intvar::special_agent_begin +
       construct::intvar::special_agent_count - 1" />

      <!-- Agent bookkeeping variables -->
      <var name="human_agent_begin" value="0" />
      <var name="agent_count" value="construct::intvar::special_agent_end  + 1" />
      <var name="human_agent_list"
        value="construct::intvar::human_agent_begin..construct::intvar::agent_count-
1" />

      <!-- ############## End Agent definitions ############## -->


      <!-- ############## Start Knowledge bits definitions ############## -->
      <var name="knowledgegroup_count" value="6" />

      <!-- General Cultural Knowledge to drive homophily-based interactions -->
      <var name="human_agent_general_knowledge_weight" value="0.3" />
      <var name="General_Cultural_Per_AOC" value="30" />
      <var name="Culture_begin" value="0" />
      <var name="Culture_end"
        value="5 * construct::intvar::General_Cultural_Per_AOC -1" />

      <var name="USAF_Culture_begin" value="0" /> <!-- 30 culture bits -->
      <var name="USAF_Culture_end"
        value="construct::intvar::USAF_Culture_begin +
       construct::intvar::General_Cultural_Per_AOC -1" />
      <var name="AFCyber_Culture_begin"
        value="construct::intvar::USAF_Culture_end + 1" />
      <var name="AFCyber_Culture_end"
        value="construct::intvar::AFCyber_Culture_begin +
        construct::intvar::General_Cultural_Per_AOC -1 " />
      <var name="Regional_Culture_begin"
        value="construct::intvar::AFCyber_Culture_end + 1" />
      <var name="Regional_Culture_end"
        value="construct::intvar::Regional_Culture_begin +
        construct::intvar::General_Cultural_Per_AOC -1" />
      <var name="Space_Culture_begin"
        value="construct::intvar::Regional_Culture_end + 1" />
      <var name="Space_Culture_end"
        value="construct::intvar::Space_Culture_begin +
        construct::intvar::General_Cultural_Per_AOC -1" />
      <var name="Strat_Culture_begin"
        value="construct::intvar::Space_Culture_end + 1" />
      <var name="Strat_Culture_end"
        value="construct::intvar::Strat_Culture_begin +
        construct::intvar::General_Cultural_Per_AOC -1" />

      <!-- Task Knowledge to drive expertise-seeking-based interaction -->
      <!-- Concept here is 30 facts per action listed in GMU's slide deck
        30 bits * 14 actions = 420 -->
      <var name="JPGOrder_size" value="420" />
      <var name="JPGOrder_begin" value="construct::intvar::Culture_end + 1"/>
      <var name="JPGOrder_end" value="construct::intvar::JPGOrder_begin+
        construct::intvar::JPGOrder_size-1"/>

      <!-- Misinformation/Knowledge to allow corruption of knowledge within
        the various organizations.  Concept here is possession of misinformation
        delays acquisition of good info, increases the time it
        takes to reach min knowledge threshold(s) and agreement within
        the org. Misinformation is limited to 1/2 of the total JPGOrder size
        and, as of Oct 11, only delivered through the special IT systems,
        mimicking integrity issues on those systems. -->
```

```
      <var name="MisInfo_begin" value="construct::intvar::JPGOrder_end + 1"/>
      <var name="MisInfo_end" value="construct::intvar::MisInfo_begin+
        construct::intvar::JPGOrder_size/2"/>
      <var name="knowledge_count" value="construct::intvar::MisInfo_end + 1" />

      <!-- #############
      End Knowledge bits definitions
      ############# -->


      <!-- Since a USAF AOC is a task oriented organization, we de-emphasize
        homophily as a motivator for interaction -->
      <var name="homophily_weight" value=".1" />
      <var name="expertise_weight" value=".4" />

      <!-- The task of interest in this experiment is diffusion of JPGOrder
        Knowledge. Weighting the JPG Order 4 times (4x) other knowledge
        will increase the probability that during any given interaction
        the JPGOrder knowledge will be the knowledge transferred -->
      <var name="JPGOrder_bit_value" value="4" />
      <var name="otherKnowledge_bit_value" value="1" />
      <var name="location_count" value="1" />

      <!-- Geographic proximity - agents tend to stay in their groups, but will seek
out expertise -->
      <var name="location_count" value="1" /> <!-- Not important -->
      <var name="JPG_distance" value="5" />
      <var name="Normal_distance" value="25" />
      <var name="Inter_AOC_distance" value="2500" />
      <var name="STD_distance_weight" value=".5" />
      <var name="Briefing_distance_weight" value="-0.5" /> <!-- Experimental, JPG
members MUCH MORE likely to interact with far-away actors during briefings. -->


      <!-- #################
        Start Interaction Params Configuration message length,
        number of interaction starts per time period, number of interaction
        receives per time period, duration of "Meetings," number of
        "Meetings" ("Meetings" are when physical proximity weighting drops,
        in this sim, to zero(0))
      ################## -->
      <var name="human_agent_min_message_length" value="2" />
      <var name="human_agent_max_message_length" value="5" />
      <var name="human_agent_min_initiations_per_timeperiod" value="2" />
      <var name="human_agent_max_initiations_per_timeperiod" value="2" />
      <var name="human_agent_min_receptions_per_timeperiod" value="2" />
      <var name="human_agent_max_receptions_per_timeperiod" value="2" />

      <!--  Strengthened the IT Systems from "5-15" to "15-30"  -->
      <var name="ITSystem_agent_min_message_length" value="15" />
      <var name="ITSystem_agent_max_message_length" value="30" />
      <var name="ITSystem_agent_min_initiations_per_timeperiod" value="40" />
      <var name="ITSystem_agent_max_initiations_per_timeperiod" value="40" />
      <var name="ITSystem_agent_min_receptions_per_timeperiod" value="40" />
      <var name="ITSystem_agent_max_receptions_per_timeperiod" value="40" />

      <!--  IT Resources  -->
      <var name="ITResource_agent_min_message_length"
        value="construct::intvar::JPGOrder_size" />
      <var name="ITResource_agent_max_message_length"
        value="construct::intvar::ITResource_agent_min_message_length*50" />
      <var name="ITResource_agent_min_initiations_per_timeperiod" value="0" />
      <var name="ITResource_agent_max_initiations_per_timeperiod" value="0" />
      <var name="ITResource_agent_min_receptions_per_timeperiod" value="0" />
      <var name="ITResource_agent_max_receptions_per_timeperiod"
        value="construct::intvar::ITSystems_count  *50" />

      <!-- JPG Briefings -->
      <!-- As of Oct '11, 2 meeetings each of duration 4.1667% of total time,
        and at 1/3 and 2/3 through simulation-->
      <var name="jpg_briefing_count" value="2" />
      <var name="JPG_briefing_duration"
        value="construct::intvar::time_count * 0.041667" />
      <var name="JPG_briefing_1_begin"
        value="construct::intvar::time_count / 3" />
      <var name="JPG_briefing_1_end"
```

```
          value="construct::intvar::JPG_briefing_1_begin +
          construct::intvar::JPG_briefing_duration" />

        <var name="JPG_briefing_2_begin"
          value="2 * construct::intvar::time_count / 3" />
        <var name="JPG_briefing_2_end"
          value="construct::intvar::JPG_briefing_2_begin +
          construct::intvar::JPG_briefing_duration" />


        <!-- Start Belief Distribution Configuration -->
        <var name="belief_test_threshold" value="0.0" />
        <var name="human_agent_belief_knowledge_weight" value="0.3" />
        <var name="ITSystem_cultural_knowledge_saturation" value="1.0" />
        <var name="special_agent_pos_belief_knowledge_weight" value="1" />
        <var name="special_agent_neg_belief_knowledge_weight" value="1" />


        </construct_vars>
        <construct_parameters>
        <!-- decide to have verbose output during initialization -->
        <!-- param values are true | false -->
        <param name="verbose_initialization" value="false" />

        <param name="default_agent_type" value="human" />
        <param name="forgetting" value="false" />
        <param name="use_mail" value="false" />
        <param name="belief_model" value="mask_mode" />

        <param name="interaction_requirements" value="disable" />
        <!-- Set communication weights. Should sum to one, and even if weighted
          toward facts, does not assure a transmitted fact is the fact desired
          by the initiating agent -->
        <param name="communicationWeightForBelief" value="0.1" />
        <param name="communicationWeightForBeliefTM" value="0.1" />
        <param name="communicationWeightForFact" value="0.5" />
        <param name="communicationWeightForKnowledgeTM" value="0.3" />
        <param name="thread_count" value="1" />

        <param name="transactive_memory" value="enable" />
        <param name="active_models"
          value="standard interaction model,standard influence model,standard belief
model"
          with="delay_interpolation" />

        <param name="active_mechanisms" value="none" />

        </construct_parameters>

        <nodes>

        <nodeclass type="agent_type" id="agent_type">
          <node id="human" title="human">
         <properties>
         <property name="canSendCommunication" value="true" />
         <property name="canReceiveCommunication" value="true" />
         <property name="canSendKnowledge" value="true" />
         <property name="canReceiveKnowledge" value="true" />
         <property name="canSendBeliefs" value="true" />
         <property name="canReceiveBeliefs" value="true" />
         <property name="canSendBeliefsTM" value="true" />
         <property name="canReceiveBeliefsTM" value="true" />
         <property name="canSendKnowledgeTM" value="true" />
         <property name="canReceiveKnowledgeTM" value="true" />
         <property name="canSendReferral" value="true" />
         <property name="canReceiveReferral" value="true" />
         <property name="communicationMechanism" value="direct" />
         </properties>
          </node>
        </nodeclass>


        <nodeclass type="agent" id="agent">
          <generator type="count" />
          <properties>
         <property name="generate_nodeclass" value="true" />
```

```
 <property name="generator_type" value="count" />
 <property name="generator_count" value="agent_count" />
  </properties>

</nodeclass>

<nodeclass type="knowledge" id="knowledge">
  <generator type="count" />
  <properties>
 <property name="generate_nodeclass" value="true" />
 <property name="generator_type" value="count" />
 <property name="generator_count" value="knowledge_count" />
  </properties>
</nodeclass>

<nodeclass type="binarytask" id="binarytask">
  <node id="btask_1" title="btask_1" />
</nodeclass>

<nodeclass type="belief" id="belief">
  <node id="b0" title="b0" />
  <node id="b1" title="b1" />
</nodeclass>

<nodeclass type="agentgroup" id="agentgroup">
  <node id="agent_grp1" title="agent_grp1" />
  <node id="agent_grp2" title="agent_grp2" />
  <node id="agent_grp3" title="agent_grp3" />
  <node id="agent_grp4" title="agent_grp4" />
</nodeclass>

<nodeclass type="knowledgegroup" id="knowledgegroup">
  <node id="general_knowledge" title="general_knowledge" />
  <node id="afcyber_knowledge" title="afcyber_knowledge" />
  <node id="strat_knowledge" title="strat_knowledge" />
  <node id="space_knowledge" title="space_knowledge" />
  <node id="regional_knowledge" title="regional_knowledge" />
  <node id="JPGOrder_knowledge" title="JPGOrder_knowledge" />
</nodeclass>



<nodeclass type="timeperiod" id="timeperiod">
  <properties>
 <property name="generate_nodeclass" value="true" />
 <property name="generator_type" value="count" />
 <property name="generator_count" value="time_count" />
  </properties>
</nodeclass>

<nodeclass type="dummy_nodeclass" id="dummy_nodeclass">
  <node id="dummy1" title="dummy1" />
</nodeclass>


<nodeclass type="location" id="location">
  <generator type="count" />

  <properties>
 <property name="generate_nodeclass" value="true" />
 <property name="generator_type" value="count" />
 <property name="generator_count" value="location_count" />
  </properties>
</nodeclass>


</nodes>

<networks>
<!-- Creates a network of agent x agent-type (e.g. agent_1, human) -->
<network id="agent type name network" src_nodeclass_type="agent"
  target_nodeclass_type="dummy_nodeclass" link_type="string"
  network_type="dense">

  <generator type="constant">
 <rows first="construct::intvar::human_agent_begin"
```

```
        last="nodeclass::agent::count_minus_one" />
        <cols first="0"
        last="nodeclass::dummy_nodeclass::count_minus_one" />
        <param name="constant_value" value="human" />
         </generator>

      </network>

      <!-- probability matrix for agents to check their email, only relevant
        if email checking is enabled (e.g. agent_1, 0.2) -->
      <network id="mail check probability network"
        src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
        link_type="float" network_type="dense">

        <generator type="randomuniform">
       <rows first="construct::intvar::human_agent_begin"
       last="nodeclass::agent::count_minus_one" />
       <cols first="0" last="nodeclass::dummy_nodeclass::count_minus_one" />
       <param name="min" value="1" />
       <param name="max" value="1" />
        </generator>

      </network>

      <!-- sets amount of turns each agent keeps mail in their mail queues, only
        relevant if email checking is enabled (e.g. agent_1, 6) -->
      <network id="mail time to live network" src_nodeclass_type="agent"
        target_nodeclass_type="dummy_nodeclass" link_type="int"
network_type="dense">

        <generator type="randomuniform">
       <rows first="construct::intvar::human_agent_begin"
       last="nodeclass::agent::count_minus_one" />
       <cols first="0" last="nodeclass::dummy_nodeclass::count_minus_one" />
       <param name="min" value="6" />
       <param name="max" value="6" />
        </generator>
      </network>



      <!--Vary the amount of knowledge bits from the baseline that an agent
        communicates per initiation per timeperiod -->
      <network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
        id="agent message complexity network" link_type="int" network_type="dense">

      <!-- No change here for humans -->
        <generator type="randomuniform">
       <rows first="0" last="nodeclass::agent::count_minus_one" />
       <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
       <param name="min" value="human_agent_min_message_length" />
       <param name="max" value="human_agent_max_message_length" />
       <param name="symmetric_flag" value="false" />
        </generator>

        <!-- Here, use the previously defined values for IT Systems
       ability to push lots of data per initiation-->
        <generator type="randomuniform">
       <rows first="construct::intvar::ITSystem_agent_begin"
       last="construct::intvar::ITSystem_agent_end" />
       <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
       <param name="min"
       value="construct::intvar::ITSystem_agent_min_message_length" />
       <param name="max"
       value="construct::intvar::ITSystem_agent_max_message_length" />
       <param name="symmetric_flag" value="false" />
        </generator>

        <!-- Here, use the previously defined values for IT Systems
       ability to push lots of data per initiation-->
      <generator type="randomuniform">
       <rows first="construct::intvar::ITResource_agent_begin"
       last="construct::intvar::ITResource_agent_end" />
       <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
       <param name="min"
       value="construct::intvar::ITResource_agent_min_message_length" />
```

```
        <param name="max"
        value="construct::intvar::ITResource_agent_max_message_length" />
        <param name="symmetric_flag" value="false" />
         </generator>

         <!-- Here, improve the ability of JPG members to push lots of
        knowledge (5 times normal) during JPG briefings-->

         <generator type="randomuniform">
        <rows first="construct::intvar::JPG_begin" last="construct::intvar::JPG_end"
/>
        <cols first="construct::intvar::JPG_briefing_1_begin"
        last="construct::intvar::JPG_briefing_1_end" />
        <param name="min"
        value="construct::intvar::human_agent_min_message_length*5" />
        <param name="max"
        value="construct::intvar::human_agent_max_message_length*5" />
        <param name="symmetric_flag" value="false" />
         </generator>

      </network>

      <!-- allows experimenter to vary the number of initiations per
        time-period for agents. -->
      <network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
        id="agent initiation count network" link_type="int"
        network_type="dense">

        <!-- human agent specific values -->
        <generator type="randomuniform">
       <rows first="0" last="nodeclass::agent::count_minus_one" />
       <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
       <param name="min"
       value="construct::intvar::human_agent_min_initiations_per_timeperiod" />
       <param name="max"
       value="construct::intvar::human_agent_max_initiations_per_timeperiod" />
       <param name="symmetric_flag" value="false" />
        </generator>

        <!-- IT System agent specific values -->
        <generator type="randomuniform">
       <rows first="construct::intvar::ITSystem_agent_begin"
       last="construct::intvar::ITSystem_agent_end" />
       <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
       <param name="min"
       value="construct::intvar::ITSystem_agent_min_initiations_per_timeperiod" />
       <param name="max"
       value="construct::intvar::ITSystem_agent_max_initiations_per_timeperiod" />
       <param name="symmetric_flag" value="false" />
        </generator>

        <!-- ITResource agent specific values, ensures resources are pull
       only, not push and not push/pull -->
        <generator type="randomuniform">
       <rows first="construct::intvar::ITResource_agent_begin"
       last="construct::intvar::ITResource_agent_end" />
       <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
       <param name="min"
       value="construct::intvar::ITResource_agent_min_initiations_per_timeperiod" />
       <param name="max"
       value="construct::intvar::ITResource_agent_max_initiations_per_timeperiod" />
       <param name="symmetric_flag" value="false" />
        </generator>

        <!-- Misinformation/Attacking Agent -->
        <generator type="randomuniform">
       <rows first="construct::intvar::special_agent_begin"
       last="construct::intvar::special_agent_end" />
       <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
       <param name="min"
       value="0" />
       <param name="max"
       value="construct::intvar::Integrity_Attacks_Per_Turn" />
       <param name="symmetric_flag" value="false" />
        </generator>
      </network>
```

```
      <!-- Belief Influence Network.... -->
      <network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
        id="beinf network" link_type="float" network_type="dense">

        <generator type="randomuniform">
       <rows first="0" last="0" />
       <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
       <param name="min" value="0.5" />
       <param name="max" value="0.8" />
       <param name="symmetric_flag" value="false" />
        </generator>

        <generator type="randomuniform">
       <rows first="construct::intvar::special_agent_begin"
       last="construct::intvar::special_agent_end" />
       <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
       <param name="min" value="0.5" />
       <param name="max" value="0.8" />
       <param name="symmetric_flag" value="false" />
        </generator>

      </network>

      <!-- Specify the knowledge per agent network -->
      <network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
        id="knowledge network" link_type="float" network_type="dense">

        <!-- All agents have general cultural knowledge -->
        <generator type="randombinary">
       <rows first="construct::intvar::human_agent_begin"
       last="nodeclass::agent::count_minus_one" />
       <cols first="construct::intvar::USAF_Culture_begin"
       last="construct::intvar::USAF_Culture_end" />
       <param name="mean" value=".25" />
       <param name="symmetric_flag" value="false" />
        </generator>

        <!-- Group-Specific Culture/Homophily -->
        <!-- Set AFCyber homophily bits -->
        <generator type="randombinary">
       <rows first="construct::intvar::AFCyber_begin"
last="construct::intvar::AFCyber_end" />
       <cols first="construct::intvar::AFCyber_Culture_begin"
last="construct::intvar::AFCyber_Culture_end" />
       <param name="mean" value=".5" />
       <param name="symmetric_flag" value="false" />
        </generator>
        <generator type="randombinary">
       <rows first="construct::intvar::AFCyber_JPG_begin"
last="construct::intvar::AFCyber_JPG_end" />
       <cols first="construct::intvar::AFCyber_Culture_begin"
last="construct::intvar::AFCyber_Culture_end" />
       <param name="mean" value=".5" />
       <param name="symmetric_flag" value="false" />
        </generator>

        <generator type="randombinary">
       <rows first="construct::intvar::Regional_begin"
last="construct::intvar::Regional_end" />
       <cols first="construct::intvar::Regional_Culture_begin"
last="construct::intvar::Regional_Culture_end" />
       <param name="mean" value=".5" />
       <param name="symmetric_flag" value="false" />
        </generator>
        <generator type="randombinary">
       <rows first="construct::intvar::Regional_JPG_begin"
last="construct::intvar::Regional_JPG_end" />
       <cols first="construct::intvar::Regional_Culture_begin"
last="construct::intvar::Regional_Culture_end" />
       <param name="mean" value=".5" />
       <param name="symmetric_flag" value="false" />
        </generator>

        <generator type="randombinary">
```

```
        <rows first="construct::intvar::Space_begin"
last="construct::intvar::Space_end" />
        <cols first="construct::intvar::Space_Culture_begin"
last="construct::intvar::Space_Culture_end" />
        <param name="mean" value=".5" />
        <param name="symmetric_flag" value="false" />
         </generator>
         <generator type="randombinary">
        <rows first="construct::intvar::Space_JPG_begin"
last="construct::intvar::Space_JPG_end" />
        <cols first="construct::intvar::Space_Culture_begin"
last="construct::intvar::Space_Culture_end" />
        <param name="mean" value=".5" />
        <param name="symmetric_flag" value="false" />
         </generator>

         <generator type="randombinary">
        <rows first="construct::intvar::Strat_begin"
last="construct::intvar::Strat_end" />
        <cols first="construct::intvar::Strat_Culture_begin"
last="construct::intvar::Strat_Culture_end" />
        <param name="mean" value=".5" />
        <param name="symmetric_flag" value="false" />
         </generator>
         <generator type="randombinary">
        <rows first="construct::intvar::Strat_JPG_begin"
last="construct::intvar::Strat_JPG_end" />
        <cols first="construct::intvar::Strat_Culture_begin"
last="construct::intvar::Strat_Culture_end" />
        <param name="mean" value=".5" />
        <param name="symmetric_flag" value="false" />
         </generator>

         <!-- Group Specific Task Knowledge -->

         <!-- Set JPG Task Knowledge as conglomeration of all task knowledge.
        NOTE: All 4 JPGs are receiving/using the same JPGOrder -->
         <generator type="randombinary">
        <rows first="construct::intvar::JPG_begin" last="construct::intvar::JPG_end"
/>
        <cols first="construct::intvar::JPGOrder_begin"
last="construct::intvar::JPGOrder_end" />
        <param name="mean" value=".65" />
        <param name="symmetric_flag" value="false" />
         </generator>

         <!-- Give small number of IT systems perfect task-oriented knowledge
        in every AOC -->
         <generator type="randombinary">
        <rows first="construct::intvar::SpecialITSys_begin"
last="construct::intvar::SpecialITSys_end" />
        <cols first="construct::intvar::JPGOrder_begin"
last="construct::intvar::JPGOrder_end" />
        <param name="mean" value="1.0" />
        <param name="symmetric_flag" value="false" />
         </generator>

         <!-- Give the mis-information/corruption/loss-of-integrity actor
        perfect possession of all bad knowledge -->
         <generator type="randombinary">
        <rows first="construct::intvar::special_agent_begin"
        last="construct::intvar::special_agent_end" />
        <cols first="construct::intvar::MisInfo_begin"
last="construct::intvar::MisInfo_end" />
        <param name="mean" value="1.0" />
        <param name="symmetric_flag" value="false" />
         </generator>

       </network>


       <network src_nodeclass_type="agent" target_nodeclass_type="agent"
         id="access network" link_type="float" network_type="dense">

         <!--  By Default, everyone can talk to everyone  -->
```

```
 <generator type="constant">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="0" last="nodeclass::agent::count_minus_one" />
<param name="constant_value" value="true" />
<param name="symmetric_flag" value="true" />
 </generator>

 <!--  BUT, ITResources and ITSystems are accessible based on a
DNS availability. First Generator sets value for ALL -->
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="construct::intvar::ITResource_agent_begin"
last="construct::intvar::ITSystem_agent_end" />
<param name="mean" value="construct::floatvar::DNS_FMC_All_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <!--  This second set of Generators sets value for "Regional"
ITResources, potentially over-riding the value set for ALL -->
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1610" last="1612" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1623" last="1623" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1628" last="1631" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1646" last="1647" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1652" last="1652" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1655" last="1655" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1657" last="1657" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1660" last="1660" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1678" last="1682" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1696" last="1704" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
```

```
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="1745" last="1827" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="2102" last="2121" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="2125" last="2125" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="2127" last="2127" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="2131" last="2131" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>
 <generator type="randombinary">
<rows first="0" last="nodeclass::agent::count_minus_one" />
<cols first="2135" last="2135" />
<param name="mean" value="construct::floatvar::DNS_FMC_Regional_Float" />
<param name="symmetric_flag" value="false" />
 </generator>

 <!--  Mis-information agent is limited to corrupting only the
special IT Systems (the ones usually thought of as having 100%
reliable information -->
 <!-- by default turn off access to everybody -->
 <generator type="constant">
<rows first="construct::intvar::special_agent_begin"
last="construct::intvar::special_agent_end" />
<cols first="0"
last="construct::intvar::SpecialITSys_begin -1" />
<param name="constant_value" value="0" />
<param name="symmetric_flag" value="true" />
 </generator>

 <!-- now set values for ALL AOCs TBMCS, variable dependent -->
 <generator type="constant">
<rows first="construct::intvar::special_agent_begin"
last="construct::intvar::special_agent_end" />
<cols first="construct::intvar::TBMCS_All_begin"
last="construct::intvar::TBMCS_All_end" />
<param name="constant_value"
value="construct::intvar::TBMCS_Attacked_All" />
<param name="symmetric_flag" value="true" />
 </generator>
 <!-- now set values for ALL AOCs GCCS, variable dependent -->
 <generator type="constant">
<rows first="construct::intvar::special_agent_begin"
last="construct::intvar::special_agent_end" />
<cols first="construct::intvar::GCCS_All_begin"
last="construct::intvar::GCCS_All_end" />
<param name="constant_value"
value="construct::intvar::GCCS_Attacked_All" />
<param name="symmetric_flag" value="true" />
 </generator>
 <!-- now set values for ALL AOCs C2PC, variable dependent -->
 <generator type="constant">
<rows first="construct::intvar::special_agent_begin"
last="construct::intvar::special_agent_end" />
```

```
 <cols first="construct::intvar::C2PC_All_begin"
 last="construct::intvar::C2PC_All_end" />
 <param name="constant_value"
 value="construct::intvar::C2PC_Attacked_All" />
 <param name="symmetric_flag" value="true" />
  </generator>
  <!-- now set values for ALL AOCs JADOCS, variable dependent -->
  <generator type="constant">
 <rows first="construct::intvar::special_agent_begin"
 last="construct::intvar::special_agent_end" />
 <cols first="construct::intvar::JADOCS_All_begin"
 last="construct::intvar::JADOCS_All_end" />
 <param name="constant_value"
 value="construct::intvar::JADOCS_Attacked_All" />
 <param name="symmetric_flag" value="true" />
  </generator>
  <!-- now set values for Regional AOCs TBMCS, variable dependent -->
  <generator type="constant">
 <rows first="construct::intvar::special_agent_begin"
 last="construct::intvar::special_agent_end" />
 <cols first="2125" last="2125" />
 <param name="constant_value"
 value="construct::intvar::TBMCS_Attacked_Regional" />
 <param name="symmetric_flag" value="true" />
  </generator>
  <!-- now set values for Regional AOCs GCCS, variable dependent -->
  <generator type="constant">
 <rows first="construct::intvar::special_agent_begin"
 last="construct::intvar::special_agent_end" />
 <cols first="2127" last="2127" />
 <param name="constant_value"
 value="construct::intvar::GCCS_Attacked_Regional" />
 <param name="symmetric_flag" value="true" />
  </generator>
  <!-- now set values for Regional AOCs C2PC, variable dependent -->
  <generator type="constant">
 <rows first="construct::intvar::special_agent_begin"
 last="construct::intvar::special_agent_end" />
 <cols first="2131" last="2131" />
 <param name="constant_value"
 value="construct::intvar::C2PC_Attacked_Regional" />
 <param name="symmetric_flag" value="true" />
  </generator>
  <!-- now set values for Regional AOCs JADOCS, variable dependent -->
  <generator type="constant">
 <rows first="construct::intvar::special_agent_begin"
 last="construct::intvar::special_agent_end" />
 <cols first="2135" last="2135" />
 <param name="constant_value"
 value="construct::intvar::JADOCS_Attacked_Regional" />
 <param name="symmetric_flag" value="true" />
  </generator>

</network>



<network src_nodeclass_type="knowledge"
  target_nodeclass_type="binarytask"
  id="binarytask requirement network" link_type="bool"
  network_type="dense">

  <generator type="randombinary">
 <rows first="0" last="nodeclass::knowledge::count_minus_one" />
 <cols first="0" last="nodeclass::binarytask::count_minus_one" />
 <param name="mean" value="0.5" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="knowledge" target_nodeclass_type="binarytask"
  id="binarytask truth network" link_type="bool" network_type="dense">
  <generator type="randombinary">
 <rows first="0" last="nodeclass::knowledge::count_minus_one" />
 <cols first="0" last="nodeclass::binarytask::count_minus_one" />
 <param name="mean" value="0.0" />
```

```
        <param name="symmetric_flag" value="false" />
          </generator>
        </network>

        <network src_nodeclass_type="agent" target_nodeclass_type="binarytask"
          id="binarytask assignment network" link_type="bool" network_type="dense">
          <generator type="randombinary">
         <rows first="0" last="nodeclass::agent::count_minus_one" />
         <cols first="0" last="nodeclass::binarytask::count_minus_one" />
         <param name="mean" value="1.0" />
         <param name="symmetric_flag" value="false" />
          </generator>
        </network>


        <!-- this allows an experimenter  to set the weight each agent gives to
          homophily per time period. With this deck, it is set to de-emphasize
homophily -->
        <network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
          id="knowledge similarity weight network" link_type="float"
          network_type="dense">
          <generator type="randomuniform">
         <rows first="0" last="nodeclass::agent::count_minus_one" />
         <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
         <param name="min" value="construct::floatvar::homophily_weight" />
         <param name="max" value="construct::floatvar::homophily_weight" />
         <param name="symmetric_flag" value="false" />
          </generator>
        </network>

        <!-- this allows an experimenter  to set the weight each agent gives to
          task-knowledge/expertise-seeking per time period. With this deck, it is set
          to emphasize task/expertise-knowledge -->
        <network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
          id="knowledge expertise weight network" link_type="float"
          network_type="dense"
        >
          <generator type="randomuniform">
         <rows first="0" last="nodeclass::agent::count_minus_one" />
         <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
         <param name="min" value="construct::floatvar::expertise_weight" />
         <param name="max" value="construct::floatvar::expertise_weight" />
         <param name="symmetric_flag" value="false" />
          </generator>
        </network>

        <network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
          id="binarytask similarity weight network" link_type="float"
          network_type="dense">
          <generator type="randomuniform">
         <rows first="0" last="nodeclass::agent::count_minus_one" />
         <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
         <param name="min" value="0.0" />
         <param name="max" value="0.0" />
         <param name="symmetric_flag" value="false" />
          </generator>
        </network>

        <!-- Allows experimenter  to weight some knowledge as more important than
          other knowledge -->
        <network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
          id="interaction knowledge weight network" link_type="float"
          network_type="dense">
          <generator type="constant">
         <rows first="0" last="nodeclass::agent::count_minus_one" />
         <cols first="0" last="nodeclass::knowledge::count_minus_one" />
         <param name="constant_value"
         value="construct::floatvar::otherKnowledge_bit_value" />
         <param name="symmetric_flag" value="false" />
          </generator>

          <generator type="constant">
         <rows first="0" last="nodeclass::agent::count_minus_one" />
         <cols first="construct::intvar::JPGOrder_begin"
         last="construct::intvar::JPGOrder_end" />
         <param name="constant_value"
```

```
 value="construct::floatvar::JPGOrder_bit_value" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<!-- Allows experimenter  to weight some knowledge as more important to
  send than other knowledge -->
<network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
  id="transmission knowledge weight network" link_type="float"
  network_type="dense">
  <generator type="constant">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::knowledge::count_minus_one" />
 <param name="constant_value"
 value="construct::floatvar::otherKnowledge_bit_value"/>
 <param name="symmetric_flag" value="false" />
  </generator>

  <generator type="constant">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="construct::intvar::JPGOrder_begin"
 last="construct::intvar::JPGOrder_end" />
 <param name="constant_value"
 value="construct::floatvar::JPGOrder_bit_value" />
 <param name="symmetric_flag" value="false" />
  </generator>

</network>

<!-- For the AOC resilient C2 sim, we will usually pay attention to
  proximity except during 'JPG Briefings.' During briefings, we'll
  turn proximity weighting off, thereby ignoring physical proximity.

  GPM:  Setting constant_value to '-.5' during JPG Briefings.
-->
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
  id="physical proximity weight network" link_type="float"
  network_type="dense">
  <!-- default to use physical proximity -->
  <generator type="constant">
 <rows first="construct::intvar::human_agent_begin"
 last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
 <param name="constant_value" value="construct::floatvar::STD_distance_weight"
/>
 <param name="symmetric_flag" value="false" />
  </generator>

  <!-- set time period for JPG Meeting 1 -->
<generator type="constant">
 <rows first="construct::intvar::human_agent_begin"
 last="nodeclass::agent::count_minus_one" />
 <cols first="construct::intvar::JPG_briefing_1_begin"
 last="construct::intvar::JPG_briefing_1_end" />
 <param name="constant_value" value="Briefing_distance_weight" />
 <param name="symmetric_flag" value="false" />
  </generator>

  <!-- set time period for JPG Meeting 2 -->
  <generator type="constant">
 <rows first="construct::intvar::human_agent_begin"
 last="nodeclass::agent::count_minus_one" />
 <cols first="construct::intvar::JPG_briefing_2_begin"
 last="construct::intvar::JPG_briefing_2_end" />
 <param name="constant_value" value="Briefing_distance_weight" />
 <param name="symmetric_flag" value="false" />
  </generator>

</network>


<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
  id="social proximity weight network" link_type="float"
  network_type="dense">
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
```

```
 <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
 <param name="min" value="0.0" />
 <param name="max" value="0.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
  id="sociodemographic proximity weight network" link_type="float"
  network_type="dense">
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
 <param name="min" value="0.0" />
 <param name="max" value="0.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="belief" target_nodeclass_type="knowledge"
  id="belief knowledge weight network" link_type="float"
  network_type="dense">

  <generator type="constant">
 <rows first="0" last="0" />
 <cols first="pos_belief_knowledge_begin0" last="pos_belief_knowledge_end0" />
 <param name="constant_value" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>

  <generator type="constant">
 <rows first="0" last="0" />
 <cols first="neg_belief_knowledge_begin0" last="neg_belief_knowledge_end0" />
 <param name="constant_value" value="-1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>

  <generator type="constant">
 <rows first="1" last="1" />
 <cols first="pos_belief_knowledge_begin1"

 last="pos_belief_knowledge_end1" />
 <param name="constant_value" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>

  <generator type="constant">
 <rows first="1" last="1" />
 <cols first="neg_belief_knowledge_begin1"
 last="neg_belief_knowledge_end1" />
 <param name="constant_value" value="-1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>


</network>

<network src_nodeclass_type="agent" target_nodeclass_type="belief"
  id="agent belief network" link_type="float" network_type="dense">
  <generator type="randomuniform">
 <rows first="construct::intvar::human_agent_begin"
 last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::belief::count_minus_one" />
 <param name="min" value="0.3" />
 <param name="max" value="0.3" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<!-- Defines the physical proximity of agents to other agents -->
<network src_nodeclass_type="agent" target_nodeclass_type="agent"
  id="physical proximity network" link_type="float"
  network_type="dense">
  <!-- default to far for every agent in the sim -->
  <generator type="constant">
 <rows first="0"
```

```
last="construct::intvar::special_agent_end" />
<cols first="0"
last="construct::intvar::special_agent_end" />
<param name="constant_value"
value="construct::intvar::Inter_AOC_distance" />
<param name="symmetric_flag" value="false" />
 </generator>

 <!--  People in the same AOC are close -->
 <generator type="constant">
<rows first="AFCyber_begin" last="AFCyber_end" />
<cols first="AFCyber_begin"   last="AFCyber_end" />
<param name="constant_value"
value="construct::intvar::Normal_distance" />
<param name="symmetric_flag" value="false" />
 </generator>

 <generator type="constant">
<rows first="Regional_begin" last="Regional_end" />
<cols first="Regional_begin" last="Regional_end" />
<param name="constant_value"
value="construct::intvar::Normal_distance" />
<param name="symmetric_flag" value="false" />
 </generator>

 <generator type="constant">
<rows first="Space_begin" last="Space_end" />
<cols first="Space_begin" last="Space_end" />
<param name="constant_value"
value="construct::intvar::Normal_distance" />
<param name="symmetric_flag" value="false" />
 </generator>

 <generator type="constant">
<rows first="Strat_begin" last="Strat_end" />
<cols first="Strat_begin" last="Strat_end" />
<param name="constant_value"
value="construct::intvar::Normal_distance" />
<param name="symmetric_flag" value="false" />
 </generator>

 <!--  Within each AOC's, everyone is far away from the JPG, but not
nearly so far as the Inter-AOC_distance. -->
 <generator type="constant">
<rows first="construct::intvar::AFCyber_begin"
last="construct::intvar::AFCyber_end" />
<cols first="AFCyber_JPG_begin"
last="AFCyber_JPG_end" />
<param name="constant_value"
value="5 * construct::floatvar::Normal_distance" />
<param name="symmetric_flag" value="true" />
 </generator>
 <generator type="constant">
<rows first="construct::intvar::Strat_begin"
last="construct::intvar::Strat_end" />
<cols first="Strat_JPG_begin"
last="Strat_JPG_end" />
<param name="constant_value"
value="5 * construct::floatvar::Normal_distance" />
<param name="symmetric_flag" value="true" />
 </generator>
 <generator type="constant">
<rows first="construct::intvar::Space_begin"
last="construct::intvar::Space_end" />
<cols first="Space_JPG_begin"
last="Space_JPG_end" />
<param name="constant_value"
value="5 * construct::floatvar::Normal_distance" />
<param name="symmetric_flag" value="true" />
 </generator>
 <generator type="constant">
<rows first="construct::intvar::Regional_begin"
last="construct::intvar::Regional_end" />
<cols first="Regional_JPG_begin"
last="Regional_JPG_end" />
<param name="constant_value"
```

```
 value="5 * construct::floatvar::Normal_distance" />
 <param name="symmetric_flag" value="true" />
  </generator>

  <!-- Within each AOC's JPG, all members are "JPG_distance"
 units apart -->
  <generator type="constant">
 <rows first="construct::intvar::AFCyber_JPG_begin"
 last="construct::intvar::AFCyber_JPG_end" />
 <cols first="construct::intvar::AFCyber_JPG_begin"
 last="construct::intvar::AFCyber_JPG_end" />
 <param name="constant_value"
 value="construct::floatvar::JPG_distance" />
 <param name="symmetric_flag" value="false" />
  </generator>
  <generator type="constant">
 <rows first="construct::intvar::Strat_JPG_begin"
 last="construct::intvar::Strat_JPG_end" />
 <cols first="construct::intvar::Strat_JPG_begin"
 last="construct::intvar::Strat_JPG_end" />
 <param name="constant_value"
 value="construct::floatvar::JPG_distance" />
 <param name="symmetric_flag" value="false" />
  </generator>
  <generator type="constant">
 <rows first="construct::intvar::Space_JPG_begin"
 last="construct::intvar::Space_JPG_end" />
 <cols first="construct::intvar::Space_JPG_begin"
 last="construct::intvar::Space_JPG_end" />
 <param name="constant_value"
 value="construct::floatvar::JPG_distance" />
 <param name="symmetric_flag" value="false" />
  </generator>
  <generator type="constant">
 <rows first="construct::intvar::Regional_JPG_begin"
 last="construct::intvar::Regional_JPG_end" />
 <cols first="construct::intvar::Regional_JPG_begin"
 last="construct::intvar::Regional_JPG_end" />
 <param name="constant_value"
 value="construct::floatvar::JPG_distance" />
 <param name="symmetric_flag" value="false" />
  </generator>

</network>

<network src_nodeclass_type="agent" target_nodeclass_type="agent"
  id="social proximity network" link_type="float"
  network_type="dense">

  <generator type="randomuniform">
 <rows first="construct::intvar::human_agent_begin"
 last="nodeclass::agent::count_minus_one" />
 <cols first="construct::intvar::human_agent_begin"
 last="nodeclass::agent::count_minus_one" />
 <param name="min" value="1.0" />
 <param name="max" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<!-- Allows experimenter  to vary the agent x agent sociodemographic network
  [mjl: use this for the service & rank differentiation later on] -->
<network src_nodeclass_type="agent" target_nodeclass_type="agent"
  id="sociodemographic proximity network" link_type="float"
  network_type="dense"
>
  <generator type="randomuniform">
 <rows first="construct::intvar::human_agent_begin"
 last="nodeclass::agent::count_minus_one" />
 <cols first="construct::intvar::human_agent_begin"
 last="nodeclass::agent::count_minus_one" />
 <param name="min" value="1.0" />
 <param name="max" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>
```

```
<!-- allows experimenter  to vary when agents are active by time period.
  Of particular use for weekends, shift work, periodic activity -->
<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
  id="agent active timeperiod network" link_type="bool"
  network_type="dense">

  <generator type="constant">
 <rows first="construct::intvar::human_agent_begin"
 last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
 <param name="constant_value" value="true" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<!-- this is set to read in the interaction sphere from gspher_fname -->
<network src_nodeclass_type="agent" target_nodeclass_type="agent"
  id="interaction sphere network" link_type="bool"
  network_type="dense">

  <generator type="csv_binarize">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::agent::count_minus_one" />
 <param name="filesystem_path" value="gsphere_fname" />
 <param name="skip_first_row" value="true" />
 <param name="csvrow" value="construct::stringvar::human_agent_list" />
 <param name="csvcol" value="construct::stringvar::human_agent_list" />
 <param name="symmetric" value="true" />
 <param name="load_style" value="sparse_to_dense_convert" />
 <param name="binarization_threshold" value="0.0" />
  </generator>


  <!--  The Misinformation Agent can talk to the Special IT Agents -->
  <generator type="constant">
 <rows first="special_agent_begin" last="special_agent_end"/>
 <cols first="SpecialITSys_begin" last="SpecialITSys_end"/>
 <param name="constant_value" value="1"/>
  </generator>

</network>
<network src_nodeclass_type="agent" target_nodeclass_type="agentgroup"
  id="agent group membership network" link_type="bool"
  network_type="dense">


  <generator type="randombinary">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::agentgroup::count_minus_one" />
 <param name="mean" value="1" />
 <param name="symmetric_flag" value="false" />
  </generator>

</network>

<network src_nodeclass_type="knowledge"
  target_nodeclass_type="knowledgegroup"
  id="fact group membership network" link_type="bool"
  network_type="dense">

  <generator type="randombinary">
 <rows first="0" last="nodeclass::knowledge::count_minus_one" />
 <cols first="0" last="nodeclass::knowledgegroup::count_minus_one" />
 <param name="mean" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>

</network>


<network src_nodeclass_type="agent" target_nodeclass_type="timeperiod"
  id="agent reception count network" link_type="int"
  network_type="dense">

  <generator type="randomuniform">
```

```
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
 <param name="min"
 value="construct::intvar::human_agent_min_receptions_per_timeperiod" />
 <param name="max"
 value="construct::intvar::human_agent_max_receptions_per_timeperiod" />
 <param name="symmetric_flag" value="false" />
  </generator>

  <generator type="randomuniform">
 <rows first="construct::intvar::ITSystem_agent_begin"
 last="construct::intvar::ITSystem_agent_end" />
 <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
 <param name="min"
 value="construct::intvar::ITSystem_agent_min_receptions_per_timeperiod" />
 <param name="max"
 value="construct::intvar::ITSystem_agent_max_receptions_per_timeperiod" />
 <param name="symmetric_flag" value="false" />
  </generator>

  <generator type="randomuniform">
 <rows first="construct::intvar::special_agent_begin"
 last="construct::intvar::special_agent_end" />
 <cols first="0" last="nodeclass::timeperiod::count_minus_one" />
 <param name="min" value="0" />
 <param name="max" value="0" />
 <param name="symmetric_flag" value="false" />
  </generator>

</network>


<network src_nodeclass_type="agent"
  target_nodeclass_type="dummy_nodeclass"
  id="agent selective attention effect network" link_type="float"
  network_type="dense" >
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="0" />
 <param name="min" value="1.0" />
 <param name="max" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
  id="knowledge priority network" link_type="unsigned int"
  network_type="dense">
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::knowledge::count_minus_one" />
 <param name="min" value="1" />
 <param name="max" value="1" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
  id="beInfluenced network" link_type="float" network_type="dense"
>
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="0" />
 <param name="min" value="0.0" />
 <param name="max" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
  id="influentialness network" link_type="float" network_type="dense"
>
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="0" />
 <param name="min" value="0.0" />
```

```
 <param name="max" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
  id="agent learning rate network" link_type="float" network_type="dense"
>
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="0" />
 <param name="min" value="1.0" />
 <param name="max" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="knowledge"
  id="learnable knowledge network" link_type="bool" network_type="dense"
>
  <generator type="randombinary">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::knowledge::count_minus_one" />
 <param name="mean" value="1.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
  id="agent forgetting rate network" link_type="float" network_type="dense"
>
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="0" />
 <param name="min" value="0.0" />
 <param name="max" value="0.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
  id="agent learn by doing rate network" link_type="float"
  network_type="dense"
>
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="0" />
 <param name="min" value="0.0" />
 <param name="max" value="0.0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
  id="agent forgetting variance network" link_type="float"
  network_type="dense"
>
  <generator type="constant">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="0" />
 <param name="constant_value" value="0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
  id="agent forgetting mean network" link_type="float" network_type="dense"
>
  <generator type="randomuniform">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="0" />
 <param name="min" value="0" />
 <param name="max" value="0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>
```

```
<!-- The "agent location network" holds the initial locations of agents -->
<!-- This network's initial condition might not matter at all, depending
  on the model being used. However, all the models require an "agent location
  network" to exist. -->
<network src_nodeclass_type="agent" target_nodeclass_type="location"
  id="agent location network" link_type="bool" network_type="dense"
>
  <generator type="constant">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::location::count_minus_one" />
 <param name="constant_value" value="true" />
  </generator>
</network>


<network src_nodeclass_type="location" target_nodeclass_type="location"
  id="location dependency network" link_type="bool" network_type="dense"
>
  <generator type="constant">
 <rows first="0" last="nodeclass::location::count_minus_one" />
 <cols first="0" last="nodeclass::location::count_minus_one" />
 <param name="constant_value" value="0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="dummy_nodeclass"
  id="agent location degree network" link_type="unsigned int"
  network_type="dense"
>
  <generator type="constant">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="0" />
 <param name="constant_value" value="1" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="location" target_nodeclass_type="knowledge"
  id="location knowledge network" link_type="bool" network_type="dense"
>
  <generator type="constant">
 <rows first="0" last="nodeclass::location::count_minus_one" />
 <cols first="0" last="nodeclass::knowledge::count_minus_one" />
 <param name="constant_value" value="0" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>

<network src_nodeclass_type="agent" target_nodeclass_type="agent"
  id="interaction network" link_type="bool" network_type="dense"
>
  <generator type="constant">
 <rows first="0" last="nodeclass::agent::count_minus_one" />
 <cols first="0" last="nodeclass::agent::count_minus_one" />
 <param name="constant_value" value="true" />
 <param name="symmetric_flag" value="false" />
  </generator>
</network>



</networks>

<transactivememory>
<network id="'knowledge transactive memory network'"
  ego_nodeclass_type="agent" src_nodeclass_type="agent"
  target_nodeclass_type="knowledge" link_type="bool" network_type="TMBool"
  associated_network="knowledge network"
>
  <generator type="perception_based">
 <ego first="0" last="nodeclass::agent::count_minus_one" />
 <alter first="0" last="nodeclass::agent::count_minus_one" />
 <transactive first="0"
 last="nodeclass::knowledge::count_minus_one" />
```

```
        <param name="false_positive_rate" value="0.0" />
        <param name="false_negative_rate" value="0.5" />
        <param name="rounding_threshold" value="0.0" />
        <param name="verbose" value="true" />
         </generator>

       </network>
       </transactivememory>

       <operations>
       <!-- Output CSV files -->

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename"
        value="knowledgeNetwork_ALL.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="all" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_000.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="1" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_025.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::time_count*0.25" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_033_Pre_JPG_Brief1.csv"
/>
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::JPG_briefing_1_begin" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename"
value="knowledgeNetwork_034_Post_JPG_Brief1.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::JPG_briefing_1_end + 1" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_050.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::time_count*0.5" />
         </parameters>
       </operation>
       <operation name="ReadGraphByName">
         <parameters>
```

```
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_066_Pre_JPG_Brief2.csv"
/>
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::JPG_briefing_2_begin" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename"
value="knowledgeNetwork_067_Post_JPG_Brief2.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::JPG_briefing_2_begin + 1" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_075.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::time_count*0.75" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_100.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::time_count-1" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_000.xml" />
        <param name="output_format" value="dynetml" />
        <param name="run" value="all" />
        <param name="time" value="1" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_025.xml" />
        <param name="output_format" value="dynetml" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::time_count*0.25" />
         </parameters>
       </operation>
       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_033_Pre_JPG_Brief1.xml"
/>
        <param name="output_format" value="dynetml" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::JPG_briefing_1_begin" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename"
value="knowledgeNetwork_034_Post_JPG_Brief1.xml" />
        <param name="output_format" value="dynetml" />
```

```
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::JPG_briefing_1_end + 1" />
         </parameters>
       </operation>
       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_050.xml" />
        <param name="output_format" value="dynetml" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::time_count*0.5" />
         </parameters>
       </operation>
       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_066_Pre_JPG_Brief2.xml"
/>
        <param name="output_format" value="dynetml" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::JPG_briefing_2_begin" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename"
value="knowledgeNetwork_067_Post_JPG_Brief2.xml" />
        <param name="output_format" value="dynetml" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::JPG_briefing_2_end + 1" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_075.xml" />
        <param name="output_format" value="dynetml" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::time_count*0.75" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'knowledge network'" />
        <param name="output_filename" value="knowledgeNetwork_100.xml" />
        <param name="output_format" value="dynetml" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::time_count-1" />
         </parameters>
       </operation>

       <!-- Output Probability of Interaction Networks -->
       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'interaction probability network'" />
        <param name="output_filename" value="prob_000.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="1" />
         </parameters>
       </operation>

       <operation name="ReadGraphByName">
         <parameters>
        <param name="graph_name" value="'interaction probability network'" />
        <param name="output_filename" value="prob_025.csv" />
        <param name="output_format" value="csv" />
        <param name="run" value="all" />
        <param name="time" value="construct::intvar::time_count*0.25" />
         </parameters>
       </operation>
```

```
    <operation name="ReadGraphByName">
      <parameters>
     <param name="graph_name" value="'interaction probability network'" />
     <param name="output_filename" value="prob_033_Pre_JPG_Brief1.csv" />
     <param name="output_format" value="csv" />
     <param name="run" value="all" />
     <param name="time" value="construct::intvar::JPG_briefing_1_begin" />
      </parameters>
    </operation>

    <operation name="ReadGraphByName">
      <parameters>
     <param name="graph_name" value="'interaction probability network'" />
     <param name="output_filename" value="prob_034_Post_JPG_Brief1.csv" />
     <param name="output_format" value="csv" />
     <param name="run" value="all" />
     <param name="time" value="construct::intvar::JPG_briefing_1_end + 1" />
      </parameters>
    </operation>

    <operation name="ReadGraphByName">
      <parameters>
     <param name="graph_name" value="'interaction probability network'" />
     <param name="output_filename" value="prob_050.csv" />
     <param name="output_format" value="csv" />
     <param name="run" value="all" />
     <param name="time" value="construct::intvar::time_count*0.5" />
      </parameters>
    </operation>
    <operation name="ReadGraphByName">
      <parameters>
     <param name="graph_name" value="'interaction probability network'" />
     <param name="output_filename" value="prob_066_Pre_JPG_Brief2.csv" />
     <param name="output_format" value="csv" />
     <param name="run" value="all" />
     <param name="time" value="construct::intvar::JPG_briefing_2_begin" />
      </parameters>
    </operation>

    <operation name="ReadGraphByName">
      <parameters>
     <param name="graph_name" value="'interaction probability network'" />
     <param name="output_filename" value="prob_067_Post_JPG_Brief2.csv" />
     <param name="output_format" value="csv" />
     <param name="run" value="all" />
     <param name="time" value="construct::intvar::JPG_briefing_2_end + 1" />
      </parameters>
    </operation>

    <operation name="ReadGraphByName">
      <parameters>
     <param name="graph_name" value="'interaction probability network'" />
     <param name="output_filename" value="prob_075.csv" />
     <param name="output_format" value="csv" />
     <param name="run" value="all" />
     <param name="time" value="construct::intvar::time_count*0.75" />
      </parameters>
    </operation>

    <operation name="ReadGraphByName">
      <parameters>
     <param name="graph_name" value="'interaction probability network'" />
     <param name="output_filename" value="prob_100.csv" />
     <param name="output_format" value="csv" />
     <param name="run" value="all" />
     <param name="time" value="construct::intvar::time_count-1" />
      </parameters>
    </operation>

    </operations>
  </construct>
```

Appendix 3 Construct Parameters File (params.csv)

```
parameter,value
Agent_Count,2137
IT_Systems_Count,474
IT_Resources_Count,58
DNS_FMC_All, 10
DNS_FMC_Regional, 10
Integrity_Attacks_Per_Turn,0
TBMCS_Attacked_All,0
TBMCS_Attacked_Regional,0
GCCS_Attacked_All,0
GCCS_Attacked_Regional,0
C2PC_Attacked_All,0
C2PC_Attacked_Regional,0
JADOCS_Attacked_All,0
JADOCS_Attacked_Regional,0
gsphere_fname,C2Res_interactionSphere.csv
```

Appendix 4 —Make Condor Directory Perl Script (makeCondorDirs.pl)

```
#! /usr/bin/perl -w

# Makes an entire directory tree for all the test cases for virtual experiments
# in the Resilient C2 project
#
# authored by: Michael Lanham
# Last Update: Sep 2011

#use strict;
use File::Path;
use File::Copy;

use constant NMC   => 0;
use constant PMC   => 7;    #Divide this by 100 in the construct deck
use constant FMC   => 10;
use constant FALSE    => 0;
use constant TRUE     => 1;
use constant NUM_RUNS => 20;

@ARGV == 0 or die "Usage: makeCondorDirs";
eval 'exec /usr/bin/perl -S $0 ${1+"$@"}'
  if 0;    #$running_under_some_shell

my @DNS_FMC = ( FMC, PMC );    #FMC=Fully Mission Capable
my @DNSAffected = ( 'R', 'A' );    #R=Regional, A=All
my @IntegrityAttacked = ( FALSE, TRUE );
my @IntegrityAffected = ( 'R',    'A' );    #R=Regional, A=All
my @ITSystemsAffected = ( 'TGCJ', 'TG', 'GC', 'CJ' );

my $file_template = "C2Res_params.csv";
my $params_file   = "params.csv";

#now iterate through the meaningful combinations of independent variables
#build a path name reflective of the combination
#adjust the params file to reflect the combination, copy adjusted params to
#path
$path = "condition_";
foreach $DNS_Status (@DNS_FMC) {
   foreach $DNSAffected (@DNSAffected) {
   foreach $IntegrityAttacked (@IntegrityAttacked) {
     foreach $IntegrityAffected (@IntegrityAffected) {
    foreach $Sys_Set (@ITSystemsAffected) {

    #First, created a output path based on the settings of the independent vars
    if ( $DNS_Status eq FMC ) {

   #     print "DNS_Status is $DNS_Status\n";
   $path .= "DNS_FMC_1_";
    }
    else {
```

```
   $path .= "DNS_FMC_0" . $DNSAffected . "_";

    }

    #    print "path is now $path\n";
    if ($IntegrityAttacked) {
   $path .= "I1" . $IntegrityAffected . $Sys_Set;
    }
    else {
   $path .= "I0";
    }

    #    print "path is now $path\n";

    # Open input file in read mode
    open INPUTFILE, "<", $file_template
     or die "Failed to open infile $file_template: $!\n";

    # Open output file in write mode
    open OUTPUTFILE, ">", $params_file
     or die "Failed to open outfile $params_file: $!\n";

    # Read the input file line by line
    while (<INPUTFILE>) {

#   print "inside input file and testing $_";
   if ( $DNS_Status eq PMC ) {
     my $old_regional_pattern = "DNS_FMC_Regional,\\s*". FMC;
     my $new_regional_pattern = "DNS_FMC_Regional, ".  PMC;
     $_ =~
    s/^$old_regional_pattern/$new_regional_pattern/g;
     if ( $DNSAffected eq 'A' ) {
    my $old_all_pattern = "DNS_FMC_All,\\s*" .  FMC;
    my $new_all_pattern = "DNS_FMC_All,\\s*" .  PMC;

    $_ =~ s/$old_all_pattern/$new_all_pattern/g;
     }
   }
   if ($IntegrityAttacked) {
     $_ =~
s/Integrity_Attacks_Per_Turn,0/Integrity_Attacks_Per_Turn,2/g;
     @ITSystems = (
    'TBMCS_Attacked_', 'GCCS_Attacked_',
    'C2PC_Attacked_',  'JADOCS_Attacked_'
     );

#   print "Sys_set is now..$Sys_Set with IntegrityAffected=$IntegrityAffected\n";
     if ( $Sys_Set eq 'TGCJ' ) {
    foreach $ITSystem (@ITSystems) {

    my $p_name = $ITSystem;
    $p_name .=
     $IntegrityAffected eq 'A'
     ? 'All'
     : 'Regional';

#    print "searching for $p_name\n";
    $_ =~ s/$p_name,0/$p_name,1/g;
    }
     }
     elsif ( $Sys_Set eq 'TG' ) {
    my $p_name = 'TBMCS_Attacked_';
    $p_name .=
   $IntegrityAffected eq 'A'
   ? 'All'
   : 'Regional';
    $_ =~ s/$p_name,0/$p_name,1/g;
    $p_name = 'GCCS_Attacked_';
    $p_name .=
   $IntegrityAffected eq 'A'
   ? 'All'
   : 'Regional';
    $_ =~ s/$p_name,0/$p_name,1/g;
     }
     elsif ( $Sys_Set eq 'GC' ) {
    my $p_name = 'GCCS_Attacked_';
```

```
    $p_name .=
   $IntegrityAffected eq 'A'
   ? 'All'
   : 'Regional';
    $_ =~ s/$p_name,0/$p_name,1/g;
    $p_name = 'C2PC_Attacked_';
    $p_name .=
   $IntegrityAffected eq 'A'
   ? 'All'
   : 'Regional';
    $_ =~ s/$p_name,0/$p_name,1/g;

     }
     elsif ( $Sys_Set eq 'CJ' ) {
    my $p_name = 'C2PC_Attacked_';
    $p_name .=
   $IntegrityAffected eq 'A'
   ? 'All'
   : 'Regional';
    $_ =~ s/$p_name,0/$p_name,1/g;
    $p_name = 'JADOCS_Attacked_';
    $p_name .=
   $IntegrityAffected eq 'A'
   ? 'All'
   : 'Regional';
    $_ =~ s/$p_name,0/$p_name,1/g;

     }
   }    #if ($IntegrityAttacked)
   print OUTPUTFILE $_;
    }    #end while loop

#    print "exiting while loop & path is now $path\n";
    close INPUTFILE;
    close OUTPUTFILE;
    if ( !-d $path ) {
    print "creating dirs for: $path\n";
   mkpath($path) or die "Failed to create $path: $!\n";
    }
    for ( my $i = 0 ; $i < NUM_RUNS ; $i++ ) {
   my $t_path = $path . "_$i";
   if ( !-d $t_path ) {
   print "\tmaking sub-directory: $t_path\n";
     mkpath($t_path)
    or die "Failed to create $t_path: $!\n";

#   $t_path = $path . "interaction";
#   mkpath($t_path)
#    or die "Failed to create $t_path: $!\n";
#   $t_path = $path . "kn";
#   mkpath($t_path)
#    or die "Failed to create $t_path: $!\n";

   }
    }
    for ( my $i = 0 ; $i < NUM_RUNS ; $i++ ) {
   my $t_path = $path . "_$i";
   print "\tcopying $params_file to $t_path\n";
   copy( $params_file, $t_path )
    or die "Failed to copy $params_file: $!\n";
    }

    $path = "condition_";
    unlink ($params_file);

     }    #foreach $Sys_Set (@ITSystemsAffected)
   }    #foreach $IntegrityAffected (@IntegrityAffected)
   }    #foreach $IntegrityAttacked (@IntegrityAttacked)
}    #foreach $DNSAffected (@DNSAffected)
}    #foreach $DNS_FMC (@DNS_FMC)
exit;
```

Appendix 5 —Make Condor Submission File Perl Script (makeCondorSubmitFile.pl)

```
#! /usr/bin/perl -w

# Makes a condor submission job file after finding all the condition_* dirs
# that hold all the params files
#
# authored by: Michael Lanham
# Last Update: Sep 2011

#use strict;
use File::Path;
use File::Copy;
use constant NMC   => 0;
use constant PMC   => 0.7;
use constant FMC   => 1;
use constant FALSE => 0;
use constant TRUE  => 1;
use constant NUM_RUNS => 20;


@ARGV == 0 or die "Usage: makeCondorSubmitFile";
eval 'exec /usr/bin/perl -S $0 ${1+"$@"}'
  if 0;    #$running_under_some_shell


my @DNS_FMC = ( FMC, PMC );    #FMC=Fully Mission Capable
my @DNSAffected = ( 'R', 'A' );    #R=Regional, A=All
my @IntegrityAttacked = ( FALSE, TRUE );
my @IntegrityAffected = ( 'R',    'A' );  #R=Regional, A=All
my @ITSystemsAffected = ( 'TGCJ', 'TG', 'GC', 'CJ' );
my $condor_file = "condor_submission_file.condor";
my %path_hash =();
my $condition_counter=1;

# Open output file in write mode
open OUTPUTFILE, ">", $condor_file
  or die "Failed to open outfile $condor_file: $!\n";

print OUTPUTFILE "
################################################################################
### DNS_FMC_1 means Domain Name Service (DNS) is Fully Mission Capable (FMC) ###
### Could also be Not Mission Capable (NMC)/Partially Mission Capable (PMC)  ###
### DNS_FMC_0A means DNS is PMC/NMC for ALL AOCs \t\t\t\t\t\t\t ###
### DNS_FMC_0R means DNS is PMC/NMC for only the Regional AOC \t\t\t\t ###
### _I0 means Integrity Attacks are NOT enabled\t\t\t\t\t\t\t\t ###
### _I1 means Integrity Attacks ARE enabled\t\t\t\t\t\t\t\t\t ###
### _I1A means Integrity Attacks ARE enabled against ALL AOCs \t\t\t\t ###
### _I1R means Integrity Attacks ARE enabled against only the Regional AOC\t ###
### _TGCJ means TBMCS, GCCS, C2PC, JADOCS are affected \t\t\t\t\t\t ###
### other combinations of TGCJ show which ITSysetms are affected \t\t\t ###
################################################################################
\n\n";

#now iterate through the meaningful combinations of independent variables
#build a path name reflective of the combination
#adjust the params file to reflect the combination, copy adjusted params to
#path

$path = "condition_";
foreach $DNS_Status (@DNS_FMC) {


   foreach $DNSAffected (@DNSAffected) {
   foreach $IntegrityAttacked (@IntegrityAttacked) {


     foreach $IntegrityAffected (@IntegrityAffected) {
    foreach $Sys_Set (@ITSystemsAffected) {

    #First, created a output path based on the settings of the independent vars
    if ( $DNS_Status eq FMC ) {
```

```
    #   print "DNS_Status is $DNS_Status\n";
       $path .= "DNS_FMC_1_";
        }
        else {
       $path .= "DNS_FMC_0" . $DNSAffected . "_";

        }

    #    print "path is now $path\n";
        if ($IntegrityAttacked) {
       $path .= "I1" . $IntegrityAffected . $Sys_Set;
        }
        else {
       $path .= "I0";
        }
        #we'll see FMC_1_I0 alot & we only need 1 condor job for it
        if ( $path_hash{$path}){
       $path_hash{$path}+=1;
        }else {
        $path_hash{$path}=1;
        print OUTPUTFILE
    "############################################################
    ### Job for experimental condition_num ". $condition_counter++ ."  $main::path
    ############################################################

    universe\t\t= vanilla
    requirements\t= ((ARCH == \"INTEL\" || ARCH==\"X86_64\") && ((OPSYS ==
\"WINNT52\") || (OPSYS == \"WINNT61\")) && (Machine =!= LastRemoteHost) && (Memory
>= 900))
    rank\t\t\t= ((Memory>=900) * (100*Mips + 20*KFlops + 4*Memory + 4*VirtualMemory))
    should_transfer_files\t= YES
    when_to_transfer_output\t= ON_EXIT_OR_EVICT
    executable\t\t\t= Construct.exe
    transfer_executable\t= true
    notification\t\t= Complete
    arguments\t\t\t= construct.xml
    output\t\t\t\t= out.\$(Process)
    error\t\t\t\t= err.\$(Process)
    log\t\t\t\t= condor.log
    initialdir\t\t\t= ".$path."_\$(Process)
    notify_user\t\t\t= merlanvp\@gmail.com
    nice_user\t\t\t= false
    transfer_input_files =
..\\common\\Construct.exe,..\\common\\construct.xml,..\\common\\C2Res_interactionSph
ere.csv,params.csv

    queue " . NUM_RUNS . "\n\n";
        }
        $path = "condition_";

        }    #foreach $Sys_Set (@ITSystemsAffected)
         }    #foreach $IntegrityAffected (@IntegrityAffected)
       }    #foreach $IntegrityAttacked (@IntegrityAttacked)
       }    #foreach $DNSAffected (@DNSAffected)
    }    #foreach $DNS_FMC (@DNS_FMC)
    close OUTPUTFILE;
    exit;
```